University of Alberta

Reliability-based Fault Tolerant Control Systems - Analysis and Design

by

Hongbin Li

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of **Doctor of Philosophy**.

Department of Electrical and Computer Engineering

Edmonton, Alberta
Fall 2007

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-33011-1
Our file Notre référence
ISBN: 978-0-494-33011-1

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

Abstract

This thesis develops a reliability-based framework for the analysis and design of Fault Tolerant Control Systems (FTCS's). The proposed reliability index is defined based on control objectives and hard deadline. For analysis purpose, a semi-Markov model is built from dynamical model, and stochastic transitions of Markov states describe degradation of system conditions among a finite set of states. This reliability index incorporates the characteristics of FTCS's, and can be used as a probabilistic criterion on overall system performance in long term.

Two reliability-based design methods are developed using this new reliability index as an optimization objective. The design difficulty lies in the fact that the index can be evaluated from a numerical procedure only but lacks analytical expressions. To address this problem, the first method considers stabilizing controller parameterization and randomized algorithm techniques to find the statistically optimal controller with respect to reliability. The second design method is based on a two-stage design scheme: A gradient-based search is first carried out on probabilistic $\mathcal{H}_\infty$ performance characteristics for reliability requirement; a sequential randomized algorithm with a weighted violation function is then developed for controller design to satisfy the required $\mathcal{H}_\infty$ performance, and its convergence is guaranteed with probability 1.

The proposed reliability index and evaluation method are based on the Markov modeling of fault occurrence and Fault Detection & Isolation (FDI) schemes. But Markov models accept only the exponential distribution, which causes a memoryless restriction. To remove this restriction, a semi-Markov description is adopted as a general model for cyclic FDI schemes. Furthermore, the reliability modeling and evaluation method are extended for this general model of FTCS's.

In the last part, a reliability monitoring scheme is developed. The reliability index is defined based on system dynamical responses and a safety boundary; FDI history data is used to update its transition characteristics and reliability model. This method provides an up-to-date reliability index as demonstrated on an aircraft model.

Acknowledgements

I sincerely thank my thesis supervisor, Prof. Qing Zhao, for her continuing support and help. Prof. Zhao introduced me to this magnificent area and always provided me valuable advice throughout my studies. Without her persistent encouragement and supervision, this project could never be completed.

I thank my oral examination committee members for their careful reading of thesis and valuable comments: Prof. N. Eva Wu, Prof. Michael Lipsett, Prof. Tongwen Chen, and Prof. Horacio Marquez. I also thank my candidacy and supervisory committee members for their evaluation and suggestions on my thesis proposal and research: Prof. Alan Lynch, Prof. Marquez, Prof. Chen, Prof. Ming J. Zuo, and Prof. Wilsun Xu.

I visited Aalborg University Esbjerg in Denmark from October 2006 to January 2007. The mentor professors, Prof. Zhenyu Yang and Prof. Youmin Zhang, spent a lot of time on reviewing my work and discussing with me on various topics. I am truly grateful to their kind help and technical suggestions, which have broadened my horizons and improved my knowledge in the fault tolerant control area.

Throughout my studies, I have received a great deal of help from colleges in the Advanced Control Systems Lab at the University of Alberta. In particular, Dr. Feng Ding and Dr. Huijun Gao have helped me on improving clarity of technical writing; Dr. Guofeng Zhang and Dr. Liqian Zhang have answered me numerous math questions. Also, I appreciate helpful discussions with Dr. Feng Tao, Dr. Danlei Chu, Mr. Jingbo Jiang, Ms. Jing Wu, Dr. Amr Pertew, Ms. Rong Zhou, Dr. Xiaorui Wang, Dr. Yang Shi, Dr. Iman Izadi, Dr. Jiandong Wang, etc. It is impossible to list all the help that I received. I thank all professors and members in this lab to create this great study and research place.

I appreciate the generous financial supports from the Natural Science and Engineering Research Council of Canada and the Department of Electrical and Computer Engineering at the University of Alberta. I thank the Educational Foundation Scholarship from Instrument Society of America, the Research Abroad Grant and travel awards from Faculty of Graduate Studies and Research, and the travel funds from the Graduate Student Association.

Table of Contents

1 Introduction 1
- 1.1 Background . . . 1
  - 1.1.1 Fault tolerant control systems . . . 1
  - 1.1.2 Reliability concepts and evaluation methods . . . 4
- 1.2 A framework of reliability-based FTCS's . . . 6
  - 1.2.1 Motivation . . . 6
  - 1.2.2 Existing results . . . 7
  - 1.2.3 Scope of the thesis . . . 8
- 1.3 Thesis outline . . . 9

2 Reliability modeling and evaluation 11
- 2.1 Introduction . . . 11
- 2.2 A reliability index . . . 12
- 2.3 System modeling . . . 13
  - 2.3.1 Markov dynamical model . . . 13
  - 2.3.2 Assumptions . . . 14
- 2.4 A semi-Markov process model for reliability evaluation . . . 15
  - 2.4.1 State definitions . . . 15
  - 2.4.2 Probabilistic parameters . . . 16
  - 2.4.3 The semi-Markov kernel . . . 18
- 2.5 An illustrative example . . . 23
- 2.6 Conclusions . . . 27

3 Probabilistic controller design via stabilizing controller parameterization 30
- 3.1 Introduction . . . 30
- 3.2 Problem formulation . . . 32
- 3.3 Preliminaries . . . 34
- 3.4 Stabilization conditions . . . 37
- 3.5 Controller parameterization . . . 40
- 3.6 Analysis of stabilizing controller set . . . 44
- 3.7 Synthesis of generator matrices . . . 47
- 3.8 An illustrative example . . . 49
- 3.9 Conclusion . . . 53

4 Two-stage controller design for MTTF 55
- 4.1 Introduction . . . 55
- 4.2 Problem formulation . . . 56
  - 4.2.1 System model . . . 56
  - 4.2.2 Control performance characterization . . . 58
  - 4.2.3 MTTF gradient . . . 59
- 4.3 Sequential randomized algorithms for state feedback control . . . 62
  - 4.3.1 Violation function and gradient computation . . . 64
  - 4.3.2 Controller design algorithm . . . 67
  - 4.3.3 Convergence result . . . 69
- 4.4 Sequential randomized algorithms for 2DOF control . . . 71
- 4.5 Output feedback control . . . 74

4.6 Example . . . 75
4.7 Conclusions . . . 79

5 Semi-Markov FDI model and reliability evaluation 80
5.1 Introduction . . . 80
5.2 Semi-Markov FDI model . . . 81
5.3 Reliability modeling . . . 83
5.4 Example . . . 87
5.5 Conclusions . . . 91

6 Reliability monitoring 92
6.1 Introduction . . . 92
6.2 Assumptions and system structure . . . 93
6.3 FDI scheme and its characterization . . . 95
6.3.1 Steady state tests . . . 95
6.3.2 Stochastic models . . . 95
6.3.3 Transition parameter estimation . . . 97
6.4 Out-crossing failure rates and hard-deadlines . . . 98
6.5 Reliability model construction . . . 98
6.6 Example . . . 101
6.6.1 Model description . . . 101
6.6.2 Performance characterization of controller and FDI . . . 102
6.6.3 Reliability evaluation . . . 104
6.7 Conclusions . . . 105

7 Conclusions and future work 107
7.1 Conclusions . . . 107
7.2 Future work . . . 109

Bibliography 111

A Semi-Markov processes 117

B Reliability calculation from semi-Markov process model 119

List of Figures

1.1 Structure of active FTCS 2
1.2 Structure of model-based FDI. 3
1.3 Logic sequence among main chapters. 9

2.1 State transition diagram of $X^{R}(t)$: (a) two fault modes; (b) four fault modes. 16
2.2 Calculation procedure of the semi-Markov kernel. 19
2.3 Control design diagram for F-14 lateral axis. 24
2.4 Transition probability and reliability function. 27
2.5 Transition probability and reliability function with improved FDI scheme. . 28
2.6 Transition probability and reliability function with improved controller. . . 29

3.1 The system structure. 33
3.2 Relationship between $\mathcal{P}$ and $\mathcal{K}$. 41
3.3 Illustration of controller generation. 41
3.4 Output trajectories when using $\hat{\mathbf{K}}^{*}$. 52
3.5 Output trajectories when using $\mathbf{K}$. 53
3.6 Compare reliability functions when using $\hat{\mathbf{K}}^{*}$ and $\mathbf{K}$. 54
3.7 MTTF of FTCS for 1000 generated stabilizing controllers. 54

4.1 Model-matching diagram. 60
4.2 Gradient search trajectory. 77
4.3 Transient responses in a regime model. 78

5.1 A sample path of the FDI process. 81
5.2 Sample paths of FDI models. 88
5.3 Transition probability and reliability curves. 90
5.4 Transition probability and reliability curves with a different FDI. 90

6.1 System structure. 94
6.2 A sample path of η_n. 96
6.3 Output trajectories. 102
6.4 The trajectories of matching errors. 102
6.5 FDI trajectory. 103
6.6 Histogram of FDI sojourn time. 103
6.7 Reliability functions comparison. 104
6.8 Comparison of transition probabilities. 105

List of Symbols

$\mathbf{1}_{\{\cdot\}}$	indicator function
A, B, C, D, E, F	system matrices
H_ζ	transition probability matrix of fault process $\zeta(t)$
H_η^k	transition matrix of $\eta(t)$ when $\zeta(t) = k$
i_{N} or (i, N), i_{N} or $(i, \mathrm{F}), \mathrm{F}$	the states of semi-Markov reliability process $X^{\mathrm{R}}(t)$
$X^{\mathrm{R}}(t)$	semi-Markov process for reliability evaluation
x, u, w, z	state, input exogenous, and performance vectors respectively
$E(\cdot)$	Expectation of a random variable
$\Pr\{\cdot\}$	probability of an event
$R(t)$	reliability function
S_1	set of plant modes
S_2	set of FDI modes
T_{hd}	hard deadline
$\mathbb{R}$	set of real numbers
$\mathbb{R}^n$	real vector space with dimension n
$\mathbb{N}$	set of non-negative integers
$\zeta(t)$	plant mode at t
$\eta(t)$	FDI mode at t
$\gamma_{ij}, \pi_j^i, w_j^i, v_j^i$	probabilistic parameters for $\zeta(t) = i$ and $\eta(t) = j$
A^T	transpose of matrix A
A^{-1}	inverse of matrix A
A^{-T}	$(A^T)^{-1}$, inverse of transpose of matrix A
$\|\cdot\|$	Euclidean norm for vectors and the largest singular value for matrices
$\|\cdot\|_\infty$	$\mathcal{H}_\infty$ norm of linear time-invariant system
$\mathcal{N}(\cdot), \mathcal{R}(\cdot)$	null and range spaces of matrices respectively
$A^\perp$	a matrix satisfies $\mathcal{N}(A^\perp) = \mathcal{R}(A)$ and $A^\perp A^{\perp T} > 0$
$\triangleq$	notation definition

Chapter 1

Introduction

1.1 Background

1.1.1 Fault tolerant control systems

Nowadays, advanced control system technologies have been applied in all kinds of processes and plants, including those with potential catastrophic effects on environment and human life. For instance, faults in chemical or nuclear plants may result in tremendous economic losses and environmental damages. This issue imposes higher reliability requirements on control systems, which brings forth a new branch of research - Fault Tolerant Control Systems (FTCS's).

Some fundamental terminologies used in FTCS's are quoted as follows [1]:

Definition 1.1 (Fault) *An unpermitted deviation of at least one characteristic property or parameter of the system from the acceptable/usual/standard conditions.*

Definition 1.2 (Failures) *Permanent interruption of a system's ability to perform a required function under specified operating conditions.*

Definition 1.3 (Fault Detection) *A binary decision making process: either the system is functioning properly, or there is a fault present in a system.*

Definition 1.4 (Fault Isolation) *Determination of kind, location and time of detection of a fault. Follows fault detection.*

Definition 1.5 (Fault Tolerance) *The ability of a controlled system to maintain control objectives, despite the occurrence of a fault. A degradation of control performance may be accepted.*

Fault detection and tolerance have been important concerns for safety-critical systems. Traditional methods for fault detection include voting, limit-checking, or spectral analysis of critical signals. When a fault occurs, system simply switches to a redundant component. These traditional methods are based on *physical redundancy*: Spare components are prepared for faults in important components, and redundant measurements are compared to detect faults. However, these methods may not be applicable in certain applications because of cost and space limitations. Therefore, *analytical redundancies* are usually adopted in FTCS's, which rely on system model and analytical relations among physical variables for fault detection and tolerance.

FTCS's can be generally classified into the following two categories: *passive* and *active* FTCS's.

(1) In *passive* FTCS's, a single controller is designed for presumed fault scenarios. Classical robust control theories can be adopted, and it is easy to implement. However, faults often make abrupt changes on system dynamics. It is difficult to design a fixed controller over such "uncertainties" of plant model, and the controller tends to be conservative [2].

(2) *Active* FTCS's are mainly composed of two subsystems: a Fault Detection & Isolation (FDI) scheme and a reconfigurable controller, as shown in Figure 1.1 [2]. Solid lines in the figure represent signal flow and dashed lines represent adaptation. The FDI scheme provides fault diagnosis information for a supervision scheme to modify the reconfigurable controller and to switch off faulty actuators and sensors.

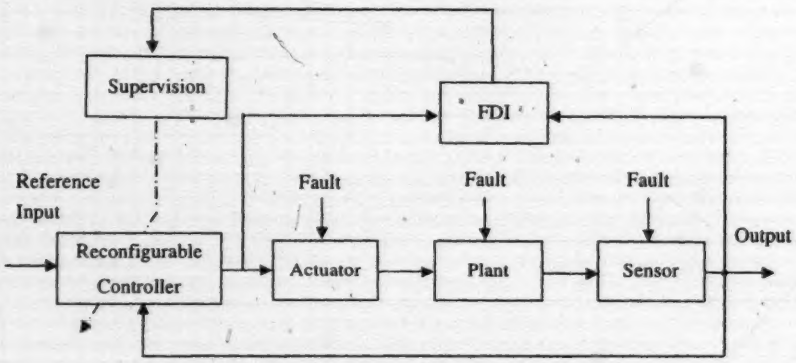

Figure 1.1: Structure of active FTCS

Most FDI schemes are designed based on the assumption of known system models, as

shown in Figure 1.2. Its main idea is to check the consistency between process measurement and corresponding estimate calculated from process model. A residual signal is generated indicating fault occurrences. Various methods can be applied for residual generation, such as observer-based design and identification-based schemes [1].

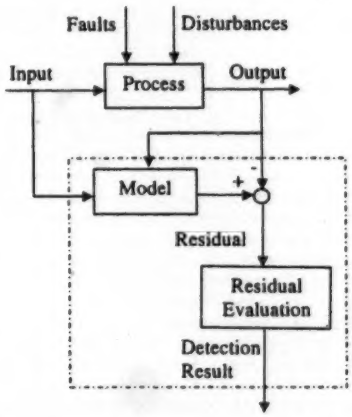

Figure 1.2: Structure of model-based FDI.

Reconfigurable control is designed to maintain acceptable control performance under fault occurrences by modifying controller according to FDI results. For example, the control law scheduling method pre-computes gain parameters for all faulty cases and switches to the corresponding gain when fault occurs [3]. In model following methods, controllers are redesigned such that system state trajectory is close to the desired one generated by an ideal model [4]. In pseudo-inverse-based methods, controller gain is adjusted to restore desired closed-loop system matrix [5].

The afore mentioned reconfigurable control methods usually require perfect information about system model and parameters for both normal and faulty cases. But modeling errors and unknown disturbances may cause imperfect decisions of FDI. Consequently, false alarms and missing detections may corrupt overall stability and performance of FTCS's [6, 7]. Many researchers have investigated this issue and proposed the so-called integrated design methods by considering the inter-relationship between FDI and reconfigurable controllers. For example, Zhang and Jiang developed an integrated FDI and reconfigurable control approach based on Interacting Multiple Model (IMM) Kalman filters and eigenvalue assignments [8]; this approach was then further improved to account for performance degradation under fault occurrences [9]. Other integrated design methods include the adaptive control based approaches [10, 11], online fault estimation and control accommodation

[12, 13], and robust control methods [14], which can be collectively categorized as deterministic Fault Tolerant Control (FTC) design approaches. In contrast, fault and FDI behaviors were modeled as two separate Markov processes in a stochastic FTC framework, in which incorrect FDI results are described as mismatched Markov states [6, 7]. Stochastic analysis and design have been performed under this modeling framework, e.g., [15, 16, 17, 18].

It has been claimed in the literature of FTCS's that reliability can be improved by FTC but very few works have investigated the reliability of FTCS's directly. Even in the so-called reliable control systems [19], the design goals are to maintain basic control performance such as stability, but no reliability index is adopted. Classical reliability assessment techniques are not geared toward the analytical redundancy in control systems. Many methods consider series-parallel or network structures but few deal with the dynamics and controller reconfigurations involved in FTCS's [20, 21, 22]. Therefore, it is difficult to relate reliability to control actions, which prevents the analysis and design from a reliability perspective.

1.1.2 Reliability concepts and evaluation methods

Definition 1.6 (Reliability[23]) *Reliability is defined as the probability of an item (a component or system) performing its intended function adequately in the specified interval of time* $[0, t]$ *under stated environmental conditions.*

To evaluate reliability, the intended functionality and associated environmental conditions need to be specified, which are often called mission profiles [24]. Reliability is computed in terms of probabilities. If the life time of an item is represented by a random variable X and its probability density function represented by $f(t)$, the cumulative probability distribution function of X is

$$F(t) \triangleq \Pr\{X \leq t\} = \int_0^t f(x)dx,$$

where $\Pr\{\cdot\}$ denotes the probability of an event. Based on Definition 1.6, reliability function $R(t)$ is the following probability:

$$R(t) \triangleq \Pr\{X > t\} = 1 - F(t) = \int_t^\infty f(x)dx. \tag{1.1}$$

Clearly, $R(0) = 1$ and $R(\infty) = 0$. (1.1) implies that reliability function $R(t)$ is the complementary cumulative probability function of life time random variable X. Or equivalently,

$$f(t) = -\frac{dR(t)}{dt}. \tag{1.2}$$

Insights on failure mechanisms can be obtained by examining failure rate or hazard function, which is defined as

$$\begin{aligned}\lambda(t) &\triangleq \lim_{\delta t \to 0} \frac{\Pr\{X \le t + \delta t | X > t\}}{\delta t} \\ &= \lim_{\delta t \to 0} \frac{\Pr\{t < X \le t + \delta t\}}{\delta t \Pr\{X > t\}} \\ &= \lim_{\delta t \to 0} \frac{R(t) - R(t + \delta t)}{\delta t R(t)} \\ &= -\frac{dR(t)}{dt}\frac{1}{R(t)} = \frac{f(t)}{R(t)}.\end{aligned}$$

As a function criterion, $R(t)$ is rarely used as an objective or constraint in design phase. An alternative scalar reliability index, Mean Time To Failure (MTTF), is usually preferable for controller or system design purpose. It is defined as the expected lifetime of satisfactory operation:

$$\text{MTTF} \triangleq E(X) = \int_0^\infty \Pr\{X > t\} dt = \int_0^\infty R(t) dt,$$

where the second equal sign is based on the fact that X is a nonnegative random variable and Theorem 1.9 in [25, p.24].

There are mainly three types of reliability evaluation methods: experimental, Monte Carlo simulation, and analytical methods [21]. A large quantity of items are tested in experimental method to estimate the distribution of life time and reliability function. Monte Carlo simulation method relies on repetitive simulated operations of physical systems for estimation. In analytical methods, mathematical models are set up to describe system operation, based on which reliability criteria are derived and calculated. This method can be further classified into the following two categories.

1) Item based method. System is decomposed into basic items from physical point of view, and their relationships are represented by reliability block diagrams, such as parallel-series or network diagrams. Reliability can be calculated based on the failure rates of critical elements in the diagram. This method may be used for feedback control systems by searching for the equivalent cut/tie sets [26]. But it is not applicable for fault detection and accommodations in FTCS's.

2) Stochastic modeling methods. System is analyzed from a functional point of view. Its operational conditions are analyzed and classified into different states, such as fully functional normal state, faulty degraded states, and failure state. System operation evolves among these states, starting from normal states, gradually jumping to

degraded states if minor faults occur and finally being absorbed in the total failure state [24]. Based on this idea, a stochastic process can be constructed with its states representing operational conditions. Reliability is then equal to the probability of this process transiting to nonfunctional failure state.

Markov process is often used to set up reliability models owing to its simplicity of calculating transition probability and hence reliability. But, its exponential sojourn time distribution imposes a restrictive memoryless property. As a result, the operation of practical systems may not be properly described. In this sense, the semi-Markov process may be suitable which allows general sojourn time distributions [25, 27].

1.2 A framework of reliability-based FTCS's

1.2.1 Motivation

It is clear that FTCS's are targeted at safety critical processes and the ultimate goal is to improve reliability [20]. However, despite being a subjective goal, reliability has hardly been used as an objective criterion that guides the design of FTCS's [22]. Available techniques are likely to restore stability and control performance under faulty conditions, but few have discussed the reliability issue directly. In this thesis, a reliability-based framework is established to conduct analysis and design.

Reliability is a widely accepted criterion in engineering systems, and it is related to different mission profiles in different systems. In control systems, closed-loop control performance objectives can be deemed as their mission profiles, and FTCS's aim to maintain them even when faults occur. The reliability concept in this sense, i.e., the probability of satisfying these control performance objectives in a given time interval with the consideration of possible faults, is consistent with controller design objective and provides a more detailed and practical description. When using reliability in this sense, control performance objectives are not lost; moreover, it gives a clear indication on how well the system will continue to satisfy these objectives considering future fault occurrences.

Classical FTC methods mainly concern with retaining stability and taking system to a safe state when faults occur in critical components. In this thesis, the reliability-based FTC methods are developed for processes under continuous long-term operation; faults may occur in many components and cause deterioration of system performance. Moreover, interruption of process operation for emergent repair may introduce high costs. Some classical FTC methods, such as FDI design and stabilization, can be used for fault diagnosis and

control design. But the focus is to achieve high reliability for non-interrupted satisfactory operation by accommodating manageable faults. Therefore, reliability-based FTC methods are more desirable than classical methods in these applications.

1.2.2 Existing results

1) An ongoing research contribution is made by Wu [12, 22, 28, 29, 30]. In this framework, overall system is decomposed into several subsystems and their functional relations and available redundancy are represented by a serial-parallel block diagram. Fault tolerance effectiveness is represented by coverage, defined as the conditional probability that system is functional when faults occur. It is used as a link between reliability indicator and control actions. By proving the monotonic dependence of reliability on coverage, it is sufficient to maximize coverage in order to obtain high system reliability. A similar system configuration was deployed in [31], where reliability was evaluated from serial-parallel structures and optimization was conducted to find the best structure based on reliability and cost. However, this framework is restricted to those FTCS's that can be described by serial-parallel block diagrams.

2) Other methods are based on Markov or semi-Markov reliability modeling. Walker proposed a semi-Markov model by defining semi-Markov states as the combinations of status of faults and FDI schemes without considering dynamical relations and control objectives [32]. Reliability evaluations from the Markov modeling of FDI were used to determine the residue threshold of FDI and to compare several sensor fault detection schemes respectively [33, 34]. Harrison, Daly, and Gai established a similar discrete-time Markov model for a redundant navigator [35]. However, in these Markov or semi-Markov models, the states are all simply defined as the combinations of fault modes and FDI results, in which the role of control on improving system performance is not considered. Hence, a link between reliability and the overall control performance of FTCS's is missing.

3) A related research area to reliability is the Fault Mode Effects Analysis (FMEA). It studies fault effect correlations and propagations among components [36]. In a large-scale system, there may be many subsystems connected together. A minor fault may cause new faults in other components and even failure of the overall system. FTCS's in this scenario should consider not only the control performance in a local subsystem but also fault propagation and overall reliability.

4) The latest progresses were reported in an invited session at the Safeprocess conference in 2006, which presented various methods of improving FTC analysis and design through an integrated reliability index. For example, a reliability-based reconfiguration strategy was developed in [37] according to an enumeration of finite system structures; a reliability index for a hierarchic diagnostic system was proposed in [38] from its functional description; Monte Carlo simulation technique was used in [39] to design an FDI scheme with high reliability; a simulation study was presented in [40] to quantify the performance of a wireless network on the effects of loop closure frequency and nodes' storage capacity; a fault diagnosis system design was discussed in [41] using reliability analysis techniques with application to a practical problem.

1.2.3 Scope of the thesis

Based on the motivation and existing results in the literature, this thesis intends to investigate the following problems:

- *How to define and to analyze the reliability of FTCS's?*

Reliability essentially provides a quantitative and probabilistic measure on the ability of a system to maintain functionality in the long run. It is particularly important for FTCS's when controlling safety-critical processes. But, control system dynamics are usually not considered in classical reliability analysis. This ignores important characteristics of FTCS's and cannot reflect true mission profiles of reliability with respect to control objectives. In addition, FTCS's contain fault detection and control reconfiguration schemes. These features need to be taken into account when defining and analyzing reliability for FTCS's.

- *How do dynamic control actions affect reliability? How to design controllers to satisfy given reliability requirement?*

Control action and reliability are on different time scales: One is usually in seconds while the other in days, months, and years. Intuitively, these two concepts are related: Well-designed controller maintains control system functionality, and therefore system can operate longer with improved reliability; in the opposite way, high reliability can be achieved only when individual components such as sensors and actuators are reliable and control system is well-designed for required control objectives. Many FTCS's and reliable control designs are performed based on this intuition, which assumes that reliability can be improved when control objectives are maintained under fault occurrences. However, it is not

clear how to quantify control effect on reliability. Designs based on intuitive assumption without quantitative analysis may not be an effective solution. If a reliability model relating controller and reliability is available, reliability-based controller design can be posed as an optimization problem.

1.3 Thesis outline

This thesis has 5 chapters, and the logical sequence is shown in Figure 1.3.

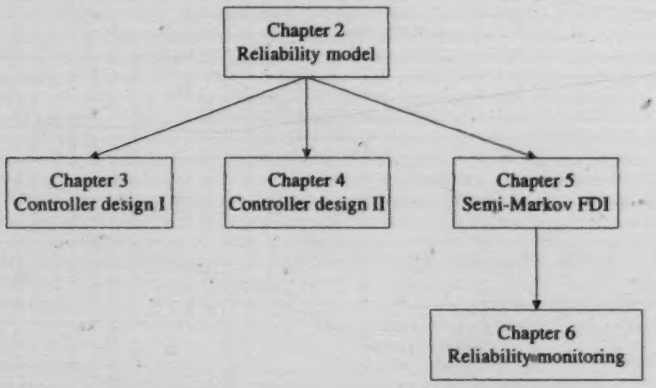

Figure 1.3: Logic sequence among main chapters.

In Chapter 2, a novel reliability index of FTCS's and its evaluation method are presented. The index is defined based on control performance and hard deadline. A semi-Markov process model is proposed to describe the operation of FTCS's for reliability evaluation. Computed from the transition probabilities of the semi-Markov process, the reliability index incorporates control objectives, performance degradation, hard deadline and the effects of imperfect FDI, an index that gives a suitable quantitative measure of overall performance.

In Chapter 3, a controller design method is discussed by considering random faults and two categories of design objectives: stability requirement and the reliability index presented in Chapter 2. A parameterization procedure together with a randomization-based optimization method is developed to find a statistically optimal controller that can stabilize the system and achieve the highest reliability.

In Chapter 4, a two-stage design scheme is developed to optimize MTTF, a long-term reliability index: A gradient-based search is first carried out on probabilistic $\mathcal{H}_\infty$ performance characteristics for MTTF requirement; a sequential randomized algorithm with a

weighted violation function is then developed for controller design to satisfy the required $\mathcal{H}_\infty$ performance, and its convergence is guaranteed with probability 1. Two iterative algorithms are carried out alternately to implement this scheme, and a controller can be designed for MTTF requirement.

In Chapter 5, the semi-Markov description of FDI is proposed, which removes the restrictive memoryless assumption in Markov models and provides a general model for cyclic FDI schemes. Furthermore, the reliability modeling of FTCS's is extended to this case.

In Chapter 6, a reliability monitoring scheme is developed for active FTCS's using results presented in Chapter 2 and 5. The history data of FDI decisions is used to update the transition characteristics of FDI and the reliability model.

The conclusions and future work are discussed in Chapter 7.

Chapter 2

Reliability modeling and evaluation*

2.1 Introduction

In order to meet high reliability requirement of safety-critical processes, major progress has been made in FTCS's [20, 28]. Existing work is mainly focused on restoring control performance under faulty conditions. However, imperfect FDI results caused by modeling uncertainties and disturbances may corrupt stability, performance, and therefore reliability [6]. So it is necessary to verify the reliability requirement of FTCS's, and quantitative reliability analysis is mandatory for safety-critical and industrial systems [42, 43]. Moreover, reliability evaluation is prerequisite to reliability-based controller design. For example, in the reliability-based design of structural control, the key problem is to evaluate the failure probability of control systems, a complementary reliability index [44]. For FTC, improving system reliability is considered to be the ultimate goal. Therefore, reliability evaluation and reliability-based FTC design have become prominent and have attracted much attention from the control community. Motivated by these considerations, the main objective of this chapter is to develop a reliability index and evaluation method for active FTCS's.

To address the effects of imperfect FDI results, Markov models are used to study the reliability evaluation problem for given FTCS. Although the Markov modeling of FDI may be restrictive, the influence of FDI imperfectness is directly tackled in this model [6, 7, 15]. The proposed reliability index incorporates the dynamical characteristics of FTCS's: control objectives, performance degradation, hard deadline, and the effects of imperfect FDI results. Based on the dynamical model of FTCS's, degraded control objectives are set for various fault scenarios, and reliability is defined as the probability of satisfying degraded objectives, while temporal violation within hard deadline is allowed. For reliability eval-

*Results presented in this chapter has been submitted to the *International Journal of Applied Mathematics and Computer Science*, revised and under review.

uation purpose, a semi-Markov process is constructed to describe and to predict control performance evolution due to fault occurrences and imperfect FDI results, and its transition probabilities are computed to determine reliability.

The remainder of this chapter is organized as follows: A reliability index is defined in Section 2.2; system model and assumptions are given in Section 2.3; a semi-Markov reliability model is presented in Section 2.4; and an example is given in Section 2.5 followed by conclusions in Section 2.6.

2.2 A reliability index

Definition 2.1 *The reliability function $R(t)$ of FTCS's is defined as the probability that, during time interval $[0, t]$, FTCS's either satisfy presumed control objectives or violate them only temporally for a short time no more than the presumed hard deadline T_{hd}.*

A reliability index is introduced in Definition 2.1 to reflect the following dynamical characteristics of FTCS's:

- Control objectives. FTCS's are said to be functional if they satisfy given control objectives. A scalar function $J(t)$ is assumed to represent control performance at time t, and small value indicates good performance. Assume that fault modes are finite, and the performance upper bound for the i-th fault mode is denoted as J^i_{max}. The control objective is to maintain $J(t) \leq J^i_{max}$ for each fault mode. More discussions are given in Section 2.3.2.

- Performance degradation. FTC deals with systems under various faulty conditions. Degraded control objectives, described by different performance bounds under various fault modes, are usually applied based on current fault mode and available system resources. For example, the performance bound under certain fault is usually higher than that of fault-free case.

- Hard deadline. Due to imperfect FDI results and control reconfigurations, $J(t)$ may exceed J^i_{max} only temporally for a short time, which should be distinguished from a failure. The hard deadline concept proposed in real-time system analysis is therefore used in Definition 2.1 [45]. It is assumed that if the violation time is greater than a particular limit T_{hd}, the system is generally unable to return to functional states. In this sense, T_{hd} is called the hard deadline of FTCS's.

Let $\zeta(t)$ represent the system fault mode at t. According to Definition 2.1, $R(t)$ is

calculated as

$$R(t) = 1 - \Pr\{\exists t_1 \in [0,t],\ t - t_1 > T_{\text{hd}},\ \forall \tau \in [t_1, t],\ J(\tau) > J^i_{\max},\ i = \zeta(\tau)\}. \quad (2.1)$$

Remark 2.1 *As an overall performance criterion of FTCS's, the reliability function $R(t)$ gives system survival probability for any operation period up to time t. The plot of calculated $R(t)$ can be deemed as a reliability prediction curve, which can be used to examine long-term system reliability behavior during offline analysis.*

The reliability evaluation problem is then reduced to developing an approach to calculate $R(t)$. The main idea is to describe the evolution of $J(t)$ using a semi-Markov process and then to calculate $R(t)$ by solving the transition probabilities of the process.

2.3 System modeling

2.3.1 Markov dynamical model

Consider the following nominal linear Markov dynamical model of FTCS's [7, 15]:

$$\mathcal{M}: \begin{cases} \dot{x}(t) = A(\zeta(t),\Delta)x(t) + B(\zeta(t),\Delta)u(\eta(t),t) + E(\zeta(t),\Delta)w(t), \\ z(t) = C(\zeta(t),\Delta)x(t) + D(\zeta(t),\Delta)w(t) + F(\zeta(t),\Delta)u(\eta(t),t), \end{cases} \quad (2.2)$$

where $x(t) \in \mathbb{R}^n, u(\eta(t),t) \in \mathbb{R}^m,\ w(t) \in \mathbb{R}^h$, and $z(t) \in \mathbb{R}^p$ denote system state, control input, exogenous input, and controlled output respectively, and $\mathbb{R}^n$ denotes real vector space with dimension n. $\zeta(t)$ and $\eta(t)$ are assumed to be two separate continuous-time Markov processes. A, B, C, D, E, F, represent system matrices with compatible dimensions, in which $\zeta(t)$ and $\eta(t)$ represent fault and FDI modes respectively, and Δ represents a vector of uncertain modeling parameters.

Based on probabilistic robustness analysis [46], modeling uncertainties Δ in (2.2) are assumed to have known probability distributions in bounded sets without specific structures. For example, they can be uncertain matrices additive to system matrices or uncertain transfer functions multiplicative to the nominal model.

The system in (2.2) can be deemed as a hybrid dynamical system including both continuous state and discrete modes [6]: The discrete modes, also referred to as system regimes, are represented by $\zeta(t)$ and $\eta(t)$ subjected to stochastic evolution, and the dynamics of continuous-state $x(t)$ is described by linear state space equations, $\mathcal{M}(\zeta(t),\eta(t))$, for the corresponding system regimes.

$\zeta(t)$ is given as a homogeneous Markov process with finite state space $S_1 = \{0, 1, \cdots, N_1\}$ to describe system fault modes, $N_1 \in \mathbb{N}$. $\mathbb{N}$ denotes the set of nonnegative integers.

The transition probability from mode i to j, $i, j \in S_1$, in the infinitesimal time interval of δt is given by

$$\zeta(t) : p_{ij}(\delta t) = \begin{cases} \alpha_{ij}\delta t + o(\delta t), \ i \neq j, \\ 1 - \alpha_{ii}\delta t + o(\delta t), \ i = j, \end{cases}$$

where α_{ij}, $\alpha_{ii} \geq 0$ are the transition rates of $\zeta(t)$, and $o(\delta t)$ denotes the high order infinitesimal.

$\eta(t)$ is given as a conditionally Markov process with finite state space $S_2 = \{0, 1, \cdots, N_2\}$ to describe FDI results, $N_2 \in \mathbb{N}$. When $\zeta(t) = k$, $k \in S_1$, the transition probability from mode i to j, $i, j \in S_2$, in δt is given by

$$\eta(t) : p_{ij}^k(\delta t) = \begin{cases} \beta_{ij}^k \delta t + o(\delta t), \ i \neq j, \\ 1 - \beta_{ii}^k \delta t + o(\delta t), \ i = j, \end{cases}$$

where β_{ij}^k, $\beta_{ii}^k \geq 0$ represent the transition rates of $\eta(t)$ given $\zeta(t) = k$. These transition rates compose the generator matrices of $\zeta(t)$ and $\eta(t)$, denoted by $H_\zeta = [\pm\alpha_{ij}]_{N_1 \times N_1}$ and $H_\eta^k = [\pm\beta_{ij}^k]_{N_2 \times N_2}$ respectively, where negative sign is taken when $i = j$.

2.3.2 Assumptions

The assumptions made in this chapter are explained as follows:

Assumption 2.1 *For the fixed system regime modes $\zeta(t)$ and $\eta(t)$, (2.2) is reduced to a linear system model $\mathcal{M}(\zeta(t), \eta(t))$. Assume that the control performance of $\mathcal{M}(\zeta(t), \eta(t))$ can be represented by a model-based static performance measure $\mu(\cdot)$.*

The term "*static*" means that $\mu(\cdot)$ depends on system model only, but not on system state trajectory $x(t)$ or output response $y(t)$. Essentially, this model-based static performance represents an average measure on how the system behaves in a particular regime. This assumption is made mainly because of the fact that a reliability index usually concerns long-term and average behavior. Average performance measure is therefore more suitable for reliability analysis. For example, $\mu(\cdot)$ can be defined as $\|G_{zw}(\zeta(t), \eta(t), s)\|$, the system norm of the transfer function from w to z of the regime model, such as $\mathcal{H}_\infty$ and $\mathcal{H}_2$ norms. With the development of robust and optimal control, system norms represent a widely-used static model-based index and have become a standard performance criterion. They can be used to describe general control objectives including trajectory tracking, disturbance attenuation, model matching, output variance when considering Gaussian disturbance, etc. As a practical example, $\mathcal{H}_\infty$ norm is used in [47] to describe a handling quality control problem in an aircraft.

Some objectives depending on system state can be converted into model-based objectives, such as the guaranteed cost control [48]. But in general, time-varying control objectives depending on system state can not be represented by $\mu(\cdot)$. For example, if the time-varying control objectives are to maintain the system state trajectory within a safety region under a Gaussian noise disturbance, $\mu(\cdot)$ is not applicable, and the methods presented in [44] can be used instead to estimate the probabilistic performance for reliability evaluation.

The performance value $J(t)$ is calculated as $\mu(\mathcal{M}(\zeta(t), \eta(t)))$. Based on Assumption 2.1, it is a constant for fixed $\zeta(t)$ and $\eta(t)$. By abuse of notation, we use $J(\zeta(t), \eta(t)) \triangleq \mu(\mathcal{M}(\zeta(t), \eta(t)))$ to denote the dependence of this performance value on system regimes.

Assumption 2.2 *The probability distribution of $\eta(t)$ can be approximated by its stationary distribution.*

This assumption is a result of the limiting probability theory of Markov processes [25]. Considering the meanings of $\zeta(t)$ and $\eta(t)$, the transition rates of $\eta(t)$ represent how fast FDI modes change for a particular fault mode while those of $\zeta(t)$ describe how frequent faults occur. As fault occurrences are often rare in practice, the transition rates of $\zeta(t)$ are usually in a smaller order than those of $\eta(t)$. So the time for FDI to approach its stationary distribution is much shorter than the mean time of fault occurrences, and this assumption is therefore made though some approximation errors may be introduced.

2.4 A semi-Markov process model for reliability evaluation

A semi-Markov process, denoted as $X^{\mathrm{R}}(t)$, is used as an intermediate model between FTCS's and the reliability index - it is constructed based on probabilistic parameters obtained from the dynamical model (2.2), and its transition probabilities are used to compute the reliability index $R(t)$ in (2.1).

2.4.1 State definitions

Two state transition diagrams are shown in Figure 2.1, where Figure 2.1.(a) is for the case of two fault modes $\{0,\ 1\}$, and Figure 2.1.(b) four fault modes $\{0,\ 1,\ 2,\ 3\}$ (in which the self-transitions of each state are not shown for the sake of clarity). $X^{\mathrm{R}}(t)$ has five states in Figure 2.1.(a), denoted by $S_{\mathrm{r}} = \{0_{\mathrm{N}},\ 0_{\mathrm{F}},\ 1_{\mathrm{N}},\ 1_{\mathrm{F}},\ \mathrm{F}\}$, and nine states in Figure 2.1.(b): 'F' represents the unique absorbing failure state, and functional states are represented by a pair with a number and a letter in the subscript. The number represents fault mode, the letter

'N' indicates satisfactory performance, and 'F' unsatisfactory performance but within the hard deadline. For $i \in S_1$, i_N and i_F are defined as

$$i_N : \{\zeta(t) = i,\ J(i,\ \eta(t)) \leq J^i_{\max}\},\ \ i_F : \{\zeta(t) = i,\ J(i,\ \eta(t)) > J^i_{\max},\ \tau \leq T_{hd})\}, \tag{2.3}$$

where τ denotes the sojourn time at i_F. Each state of $X^R(t)$ indicates fault mode and whether or not the control objective is satisfied. By studying the state transitions of $X^R(t)$, performance evolution and reliability can be analyzed.

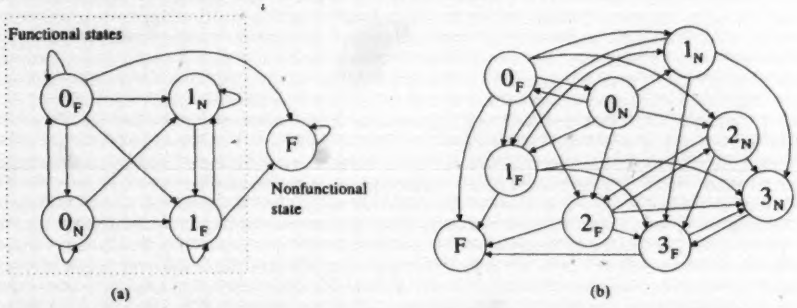

Figure 2.1: State transition diagram of $X^R(t)$: (a) two fault modes; (b) four fault modes.

2.4.2 Probabilistic parameters

Considering modeling uncertainties, control performance can be given in terms of a classical worst-case measure for robustness but it may lead to a conservative result. In contrast, probabilistic robustness analysis assumes a probability distribution of parametric uncertainties and evaluates the probability of satisfying a specific performance using randomized algorithms [46]. This alternative criterion has clear meaning in practice where the required performance objectives are always associated with certain minimum probability levels [49]. Following this idea, the following parameter is defined:

Definition 2.2 *For a particular fault mode and FDI mode, the probability that the system is functional is defined as*

$$\begin{aligned} \gamma_{ij} &\triangleq \Pr\{J(\zeta(t),\ \eta(t)) \leq J^i_{\max} | \zeta(t) = i,\ \eta(t) = j\} \\ &= \Pr\{J(i,j) \leq J^i_{\max}\} \\ &= \Pr\{\mu(\mathcal{M}(i,j)) \leq J^i_{\max}\}, \end{aligned} \tag{2.4}$$

where $i \in S_1,\ j \in S_2$.

γ_{ij} is the probabilistic performance when the fault mode is i and FDI mode is j. Based on Assumption 2.1, γ_{ij} can be estimated using randomized algorithm given by [46].

Remark 2.2 *γ_{ij} is a key parameter connecting the control performance of a particular system regime and the reliability of FTCS's. It demonstrates the influence of system dynamics and controllers on the reliability index $R(t)$.*

Definition 2.3 *For a particular fault mode, the stationary distribution of the FDI mode is defined as*

$$\pi_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j | \zeta(t) = i\},\ \ i \in S_1,\ \ j \in S_2.$$

π_j^i can be calculated based on the generator matrix of $\eta(t)$ when $\zeta(t) = i$ [25]. Based on Assumption 2.2, π_j^i is used to approximate the following probability:

$$\Pr\{\eta(t) = j | \zeta(t) = i\} \approx \pi_j^i,\ \ i \in S_1,\ \ j \in S_2. \tag{2.5}$$

Remark 2.3 *π_j^i reflects the detection precision of FDI. In the ideal case of perfect FDI detection, $\pi_j^i = 0$ when $i \neq j$ and $\pi_i^i = 1$. So this parameter gives a probabilistic measure on FDI imperfectness.*

Definition 2.4 *Given $X^R(t) = i_N$, $i \in S_1$, the stationary probability that the FDI process equals a specific mode is defined as*

$$w_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j | X^R(t) = i_N\},\ \ i \in S_1,\ \ j \in S_2.$$

w_j^i can be computed based on the Bayes' formula as shown below in the example of w_0^0 in the case of $S_2 = \{0,\ 1\}$. If γ_{00} and γ_{01} are not equal to zero simultaneously, then

$$\begin{aligned}
w_0^0 &= \lim_{t\to\infty} \Pr\{\eta(t) = 0 | X^R(t) = 0_N\} = \lim_{t\to\infty} \Pr\{\eta(t) = 0 | \zeta(t) = 0,\ J(0,\eta(t)) \le J_{\max}^0\} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(t) \le J_{\max}^0 | \eta(t) = 0,\ \zeta(t) = 0\} \Pr\{\eta(t) = 0,\ \zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(t) \le J_{\max}^0 | \eta(t) = k,\ \zeta(t) = 0\} \Pr\{\eta(t) = k,\ \zeta(t) = 0\}} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(0,\eta(t)) \le J_{\max}^0 | \eta(t) = 0\} \Pr\{\eta(t) = 0 | \zeta(t) = 0\} \Pr\{\zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(0,\eta(t)) \le J_{\max}^0 | \eta(t) = k\} \Pr\{\eta(t) = k | \zeta(t) = 0\} \Pr\{\zeta(t) = 0\}} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(t) \le J_{\max}^0 | \eta(t) = 0,\ \zeta(t) = 0\} \Pr\{\eta(t) = 0 | \zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(t) \le J_{\max}^0 | \eta(t) = k,\ \zeta(t) = 0\} \Pr\{\eta(t) = k | \zeta(t) = 0\}} \\
&= \frac{\Pr\{J(0,0) \le J_{\max}^0\} \lim_{t\to\infty} \Pr\{\eta(t) = 0 | \zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(0,k) \le J_{\max}^0\} \lim_{t\to\infty} \Pr\{\eta(t) = k | \zeta(t) = 0\}} \\
&= \frac{\gamma_{00}\pi_0^0}{\gamma_{00}\pi_0^0 + \gamma_{01}\pi_1^0}.
\end{aligned} \tag{2.6}$$

Considering that all cases of $\eta(t) = k$ form a partition of event space, $k \in S_2$, Bayes's formula is used in the second line of the above derivations, where the conditional probability

is converted to known mariginal and other conditional probabilities. If $\gamma_{00} = \gamma_{01} = 0$, w_{00} is defined as π_0^0. The calculation procedures are similar for other values of i and j.

Definition 2.5 *Given $X^R(t) = i_F$, $i \in S_1$, the stationary probability that the FDI process equals a specific mode is defined as*

$$v_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j | X^R(t) = i_F\}, \quad i \in S_1, \quad j \in S_2.$$

v_j^i can be calculated in a similar way as w_j^i.

Based on Assumption 2.2 and (2.5), w_j^i and v_j^i are used to approximate the following probabilities:

$$\Pr\{\eta(t) = j | X^R(t) = i_N\} \approx w_j^i, \quad \Pr\{\eta(t) = j | X^R(t) = i_F\} \approx v_j^i, \quad i \in S_1, \quad j \in S_2. \tag{2.7}$$

Remark 2.4 *w_j^i and v_j^i are probabilistic estimates of FDI modes given the states of $X^R(t)$, and determined by the control performance of each system regime and FDI imperfectness parameters, represented by γ_{ij} and π_j^i respectively.*

2.4.3 The semi-Markov kernel

The associated Markov-renewal process of $X^R(t)$ is denoted by $(Y_n, T_n, n \in \mathbb{N})$. Y_n denotes the so-called embedded Markov chain, which gives the state sequence visited by $X^R(t)$ consecutively, and T_n the transition time. The semi-Markov kernel of $X^R(t)$ is denoted by a matrix function Q, and its element gives one-step transition probability. For example, $Q(i_N, j_N, t)$ is defined in the following equation, $i_N, j_N \in S_r, t \in \mathbb{R}, t \geq 0$:

$$Q(i_N, j_N, t) \triangleq \Pr\{Y_{n+1} = j_N, T_{n+1} - T_n \leq t | Y_n = i_N\},$$

the probability of transiting from i_N to j_N in one step with sojourn time $T_{n+1} - T_n$ no greater than t [25].

According to Assumption 2.1, the state transitions of $X^R(t)$ are triggered by the mode changes of $\zeta(t)$ or $\eta(t)$, implying that faults, FDI decisions, and controller reconfigurations have major effects on system performance and reliability. Hence the semi-Markov kernel Q is essential for reliability evaluation. By taking the transition of $X^R(t)$ from 0_N in Figure 2.1.(a) as an example, the main steps of calculating Q are listed as follows and illustrated in Figure 2.2.

1) The FDI mode $\eta(t)$ before transition is estimated using w_j^i or v_j^i based on the state of $X^{\mathrm{R}}(t)$.

2) Competition between $\zeta(t)$ and $\eta(t)$. The process that jumps first determines possible transitional destination states. For example, if $\zeta(t)$ jumps before $\eta(t)$, the destination state is 1_{N} or 1_{F}; otherwise, 0_{N} or 0_{F}. This competition probability can be calculated using a property of exponential distributions.

3) The probability of satisfying control objectives at destination states is calculated by using γ_{ij}.

4) By combining previous steps, the transition probability is calculated using the total probability formula.

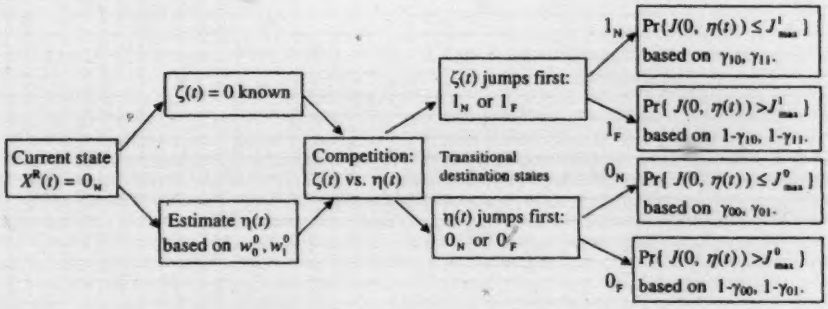
Current state
$X^R(t) = 0_N$
$\zeta(t) = 0$ known
Estimate $\eta(t)$ based on w_0^0, w_1^0
Competition: $\zeta(t)$ vs. $\eta(t)$
$\zeta(t)$ jumps first: 1_N or 1_F
$\eta(t)$ jumps first: 0_N or 0_F
Transitional destination states
1_N
1_F
0_N
0_F
Pr{ $J(0, \eta(t)) \le J^1_{max}$ } based on γ_{10}, γ_{11}.
Pr{ $J(0, \eta(t)) > J^1_{max}$ } based on $1-\gamma_{10}, 1-\gamma_{11}$.
Pr{ $J(0, \eta(t)) \le J^0_{max}$ } based on γ_{00}, γ_{01}.
Pr{ $J(0, \eta(t)) > J^0_{max}$ } based on $1-\gamma_{00}, 1-\gamma_{01}$.

Figure 2.2: Calculation procedure of the semi-Markov kernel.

The property of exponential distributions mentioned in step 2) is given as follows:

Let $X_1, \cdots, X_n$ be independent random variables, with X_i following an exponential distribution with parameter λ_i, $i = 1 \sim n$. Then the distribution of $\min(X_1, \cdots, X_n)$ is still exponentially distributed with parameter $(\lambda_1 + \cdots + \lambda_n)$, and the probability of X_i being the minimum is $\lambda_i/(\lambda_1 + \cdots + \lambda_n)$, $i = 1 \sim n$.

For example, suppose $\zeta(t) = 0$ and $\eta(t) = 0$ before transition. Let τ_ζ denote the sojourn time of $\zeta(t)$, and τ_η the sojourn time of $\eta(t)$. Because of Markov process theory, τ_ζ and τ_η are exponentially distributed with parameters given in the generator matrix:

$$\Pr\{\tau_\zeta \le t\} = 1 - e^{-\alpha_{00} t}, \quad \Pr\{\tau_\eta \le t\} = 1 - e^{-\beta_{00}^0 t}.$$

Based on the above property,

$$\Pr\{\min(\tau_\zeta, \tau_\eta) \le t\} = 1 - e^{-(\alpha_{00} + \beta_{00}^0) t},$$

$$\Pr\{\tau_\zeta < \tau_\eta\} = \frac{\alpha_{00}}{\alpha_{00} + \beta^0_{00}},$$

$$\Pr\{\tau_\eta < \tau_\zeta\} = \frac{\beta^0_{00}}{\alpha_{00} + \beta^0_{00}}.$$

The event $\tau_\zeta < \tau_\eta$ corresponds to $\zeta(t)$ transits before $\eta(t)$, and $\tau_\eta < \tau_\zeta$ means $\eta(t)$ transits first. This event appears to be a competition between two processes, and therefore the term competition probability is used. The above three probabilities determine the competition result and are used in calculating transition probabilities to different destination states, as shown in (5.18) in the proof of Theorem 2.1.

Following the similar idea shown in Figure 2.2, the general results on calculating semi-Markov kernel are given as follows:

Theorem 2.1 *The semi-Markov kernel of $X^R(t)$ can be calculated by the following equations:*

$$Q(i_{\rm N},\, j_{\rm N},\, t) = \begin{cases} \sum\limits_{k\in S_2} w^i_k \sum\limits_{l\in S_2\backslash k} \dfrac{\beta^i_{kl}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})t})\gamma_{il}, & j = i, \\ \sum\limits_{k\in S_2} w^i_k \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})t})\gamma_{jk}, & j \in S_1\backslash i, \end{cases} \tag{2.8}$$

$$Q(i_{\rm N},\, j_{\rm F},\, t) = \begin{cases} \sum\limits_{k\in S_2} w^i_k \sum\limits_{l\in S_2\backslash k} \dfrac{\beta^i_{kl}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})t})(1-\gamma_{il}), & j = i, \\ \sum\limits_{k\in S_2} w^i_k \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})t})(1-\gamma_{jk}), & j \in S_1\backslash i, \end{cases} \tag{2.9}$$

$$Q(i_{\rm F},\, j_{\rm N},\, t) = \begin{cases} \sum\limits_{k\in S_2} v^i_k \sum\limits_{l\in S_2\backslash k} \dfrac{\beta^i_{kl}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})\min(t,T_{\rm hd})})\gamma_{il}, & j = i, \\ \sum\limits_{k\in S_2} v^i_k \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})\min(t,T_{\rm hd})})\gamma_{jk}, & j \in S_1\backslash i, \end{cases} \tag{2.10}$$

$$Q(i_{\rm F},\, j_{\rm F},\, t) = \begin{cases} \sum\limits_{k\in S_2} v^i_k \sum\limits_{l\in S_2\backslash k} \dfrac{\beta^i_{kl}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})\min(t,T_{\rm hd})})(1-\gamma_{il}), & j = i, \\ \sum\limits_{k\in S_2} v^i_k \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta^i_{kk}}(1-e^{-(\alpha_{ii}+\beta^i_{kk})\min(t,T_{\rm hd})})(1-\gamma_{jk}), & j \in S_1\backslash i, \end{cases} \tag{2.11}$$

$$Q(i_{\rm F},\, {\rm F},\, t) = \mathbf{1}_{\{t>T_{\rm hd}\}}(1-\sum_{j\in S_1}(Q(i_{\rm F},\, j_{\rm N},\, T_{\rm hd}) + Q(i_{\rm F},\, j_{\rm F},\, T_{\rm hd}))), \tag{2.12}$$

$$Q({\rm F},\, {\rm F},\, t) = 1,\ Q({\rm F},\, j_{\rm N},\, t) = Q({\rm F},\, j_{\rm F},\, t) = 0,\ j \in S_1, \tag{2.13}$$

where $t > 0$, $i, j \in S_1$, $S_2\backslash k \triangleq \{a | a \in S_2,\ a \neq k\}$, and $S_1\backslash i \triangleq \{b | b \in S_1,\ b \neq i\}$. S_1, S_2, and $S_{\rm r}$ denote the state spaces of $\zeta(t)$, $\eta(t)$, and $X^{\rm R}(t)$ respectively. The indicator function $\mathbf{1}_{\{t>T_{\rm hd}\}} = 1$ if $t > T_{\rm hd}$; otherwise, $\mathbf{1}_{\{t>T_{\rm hd}\}} = 0$.

Proof: By applying the total probability formula and conditioning the probability on FDI modes, the first case of (2.8) can be decomposed into three parts as shown in the following equation, where (Y_n, T_n) denotes the associated Markov renewal process of $X^{\mathrm{R}}(t)$:

$$
\begin{aligned}
& Q(i_{\mathrm{N}},\, i_{\mathrm{N}},\, t) \triangleq \Pr\{Y_{n+1} = i_{\mathrm{N}},\, T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}}\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \Pr\{Y_{n+1} = i_{\mathrm{N}},\, T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}},\, \eta(T_n) = k\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \Pr\{J(i, \eta(T_{n+1})) \le J^i_{\max},\, \zeta(T_{n+1}) = i, \\
& T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}},\, \eta(T_n) = k\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \sum_{l \in S_2 \backslash k} \Pr\{\zeta(T_{n+1}) = i,\, \eta(T_{n+1}) = l, \\
& T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}},\, \eta(T_n) = k\} \Pr\{J(i,\, \eta(T_{n+1})) \le J^i_{\max} | \zeta(T_{n+1}) = i, \\
& \eta(T_{n+1}) = l,\, T_{n+1} - T_n \le t, Y_n = i_{\mathrm{N}},\, \eta(T_n) = k\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \sum_{l \in S_2 \backslash k} \Pr\{\zeta(T_{n+1}) = i,\, \eta(T_{n+1}) = l, \\
& T_{n+1} - T_n \le t | \zeta(T_n) = i,\, \eta(T_n) = k\} \Pr\{J(i,\, l) \le J^i_{\max}\}. \qquad (2.14)
\end{aligned}
$$

The first and last terms in (2.14) can be approximated by the corresponding stationary probabilities:

$$
\Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \approx w^i_k,\;\; \Pr\{J(i,\, l) \le J^i_{\max}\} \approx \gamma_{il}. \qquad (2.15)
$$

The second term in (2.14) is equal to the competition probability:

$$
\begin{aligned}
& \Pr\{\zeta(T_{n+1}) = i,\, \eta(T_{n+1}) = l,\, T_{n+1} - T_n \le t | \zeta(T_n) = i,\, \eta(T_n) = k\} \\
= & \frac{\beta^i_{kl}}{\alpha_{ii} + \beta^i_{kk}} (1 - e^{-(\alpha_{ii} + \beta^i_{kk})t}). \qquad (2.16)
\end{aligned}
$$

Substitute (2.15)-(2.16) to (2.14), and the first case of (2.8) follows. The second case of (2.8) can be proved in similar procedure considering that the mode of $\zeta(t)$ changes instead

and the derivation is given as follows:

$$
\begin{aligned}
& Q(i_{\mathrm{N}}, j_{\mathrm{N}}, t) \triangleq \Pr\{Y_{n+1} = j_{\mathrm{N}}, T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}}\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \Pr\{J(j, \eta(T_{n+1})) \le J^j_{\max}, \zeta(T_{n+1}) = j, \\
& T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}}, \eta(T_n) = k\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \Pr\{\zeta(T_{n+1}) = j, \eta(T_{n+1}) = k, \\
& T_{n+1} - T_n \le t | Y_n = i_{\mathrm{N}}, \eta(T_n) = k\} \Pr\{J(j, \eta(T_{n+1})) \le J^j_{\max} | \zeta(T_{n+1}) = j, \\
& \eta(T_{n+1}) = k, T_{n+1} - T_n \le t, Y_n = i_{\mathrm{N}}, \eta(T_n) = k\} \\
= & \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\mathrm{N}}\} \Pr\{\zeta(T_{n+1}) = j, \eta(T_{n+1}) = k, \\
& T_{n+1} - T_n \le t | \zeta(T_n) = i_{\mathrm{N}}, \eta(T_n) = k\} \Pr\{J(j, k) \le J^j_{\max}\} \\
= & \sum_{k \in S_2} w^i_k \frac{\alpha_{ij}}{\alpha_{ii} + \beta^i_{kk}} (1 - e^{-(\alpha_{ii} + \beta^i_{kk})t}) \gamma_{jk}, \quad j \in S_1 \backslash i. \qquad (2.17)
\end{aligned}
$$

The proof of (2.9) is similar and the details are omitted.

For (2.10)-(2.12), $X^{\mathrm{R}}(t)$ transits from i_{F}, and these probabilities depend on T_{hd}. If $t \le T_{\mathrm{hd}}$, they can be calculated in a similar way as that of i_{N}; if $t > T_{\mathrm{hd}}$, $Q(i_{\mathrm{F}}, j_{\mathrm{N}}, t)$ and $Q(i_{\mathrm{F}}, j_{\mathrm{F}}, t)$ maintain the constant values of $Q(i_{\mathrm{F}}, j_{\mathrm{N}}, T_{\mathrm{hd}})$ and $Q(i_{\mathrm{F}}, j_{\mathrm{F}}, T_{\mathrm{hd}})$ respectively while $X^{\mathrm{R}}(t)$ transits to F. Therefore, (2.10)-(2.11) have similar expressions as (2.8)-(2.9) with t replaced by $\min(t, T_{\mathrm{hd}})$ [50]. $Q(i_{\mathrm{F}}, \mathrm{F}, t)$ becomes nonzero only if $t > T_{\mathrm{hd}}$, and it is complementary to the transition probability from i_{F} to other states within T_{hd}. The indicator function $\mathbf{1}_{\{t > T_{\mathrm{hd}}\}}$ describes this behavior, and (2.12) follows. (2.13) is obvious considering that F is absorbing. ■

In the above derivation, each element of semi-Markov kernel is decomposed into three parts: FDI mode estimation, competition probability, and probabilistic performance estimation, and each part can be approximated or calculated using the probabilistic parameters. The effects of hard deadline are described by $\min(t, T_{\mathrm{hd}})$ and $\mathbf{1}_{\{t > T_{\mathrm{hd}}\}}$.

Once the semi-Markov kernel is established, $R(t)$ and other reliability criteria, such as Mean Time To Failure (MTTF), are readily computed [27]. Considering that the state F is absorbing, if the initial state is 0_{N}, the reliability function $R(t) = 1 - P(0_{\mathrm{N}}, \mathrm{F}, t)$, where the transition probability function from 0_{N} to F is denoted by $P(0_{\mathrm{N}}, \mathrm{F}, t) \triangleq \Pr\{X^{\mathrm{R}}(t) = \mathrm{F} | X(0) = 0_{\mathrm{N}}\}$. Compared with $Q(0_{\mathrm{N}}, \mathrm{F}, t)$, $P(0_{\mathrm{N}}, \mathrm{F}, t)$ may involve multiple transitions but $Q(0_{\mathrm{N}}, \mathrm{F}, t)$ is for one transition only.

The main procedure of evaluating reliability for FTCS's is summarized as follows:

1) Given the Markov model (2.2) of FTCS's, the states of $X^{\mathrm{R}}(t)$ are defined as in Section 2.4.1 to reflect degraded control performance under each fault mode.

2) Continuous-state dynamics analysis. For fixed $\zeta(t)$ and $\eta(t)$, the system in (2.2) is reduced to $\mathcal{M}(\zeta(t), \eta(t))$, and the robust control performance of this regime model under probabilistic uncertainties is represented by a probabilistic parameter γ_{ij} in Definition 2.4.

3) Discrete-mode dynamics analysis. FDI imperfectness and its relations with the states of $X^{\mathrm{R}}(t)$ are described by the probabilistic parameters in Definition 2.3 through 2.5.

4) The continuous-state and discrete-mode dynamics are combined to construct the semi-Markov kernel of $X^{\mathrm{R}}(t)$ using Theorem 2.1, and $R(t)$ is calculated by solving the transition probabilities of $X^{\mathrm{R}}(t)$.

2.5 An illustrative example

A control problem of F-14 aircraft was presented in [47], and also used as a demonstration example in MATLAB® Robust Control Toolbox[1]. This problem considers the design of a lateral-directional axis controller during powered approach to a carrier landing with two command inputs from the pilot: lateral stick and rudder pedal. At an angle-of-attack of 10.5 degree and airspeed of 140 knots, the nominal linearized F-14 model has four states: lateral velocity, yaw rate, roll rate, and roll angle, denoted by v, r, p, and ϕ respectively; two control inputs, differential stabilizer deflection and rudder deflection, denoted by δ_{dstab} and δ_{rud} respectively; and four outputs: roll rate, yaw rate, lateral acceleration, and side-slip angle, denoted by p, r, y_{ac}, and β respectively. These variables are related by the following state-space equations:

$$\dot{x}_{\text{F14}} = A_{\text{F14}}x_{\text{F14}} + B_{\text{F14}}u_{\text{F14}},\ \ y_{\text{F14}} = C_{\text{F14}}x_{\text{F14}} + D_{\text{F14}}u_{\text{F14}},$$

where $x_{\text{F14}} = [v\ r\ p\ \phi]^T$, $u_{\text{F14}} = [\delta_{\text{dstab}}\ \delta_{\text{rud}}]^T$, $y_{\text{F14}} = [\beta\ p\ r\ y_{\text{ac}}]^T$, and

$$A_{\text{F14}} = \begin{bmatrix} -0.1160 & -227.2806 & 43.0223 & 31.6347 \\ 0.0027 & -0.2590 & -0.1445 & 0 \\ -0.0211 & 0.6703 & -1.3649 & 0 \\ 0 & 0.1853 & 1.0000 & 0 \end{bmatrix}, B_{\text{F14}} = \begin{bmatrix} 0.0622 & 0.1013 \\ -0.0053 & -0.0112 \\ -0.0467 & 0.0036 \\ 0 & 0 \end{bmatrix}.$$

[1] MATLAB and Robust Control Toolbox are the trademarks of The MathWorks, Inc.

$$C_{\text{F14}} = \begin{bmatrix} 0.2469 & 0 & 0 & 0 \\ 0 & 0 & 57.2958 & 0 \\ 0 & 57.2958 & 0 & 0 \\ -0.0028 & -0.0079 & 0.0511 & 0 \end{bmatrix}, \; D_{\text{F14}} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0.0029 & 0.0023 \end{bmatrix}.$$

The control objectives are to have handling quality (HQ) responses from lateral stick to roll rate p and from rudder pedal to side-slip angle β match the first- and second-order responses respectively: $5\frac{2}{s+2}$ and $-2.5\frac{1.25^2}{s+2.5s+1.25^2}$.

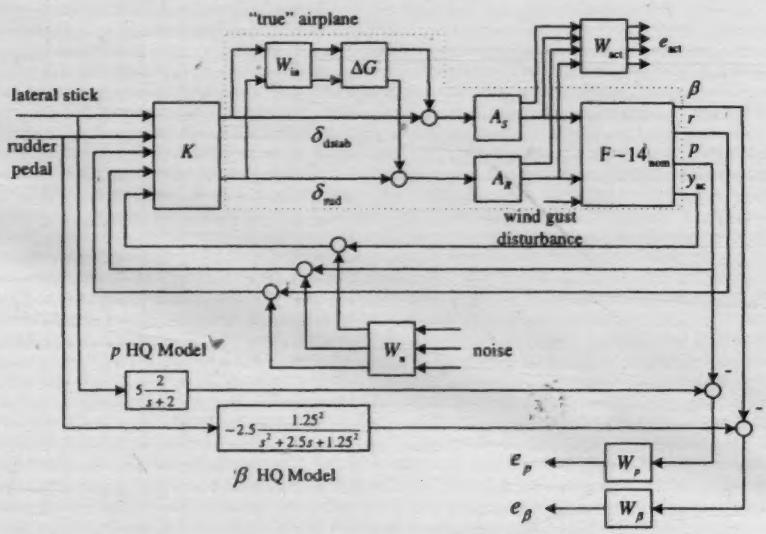

Figure 2.3: Control design diagram for F-14 lateral axis.

The system block diagram is shown in Figure 2.3, where F-14$_{\text{nom}}$ represents the nominal linearized F-14 model, and A_S and A_R actuator models. e_p and e_β represent the weighted model matching errors. Actuator energy is described by e_{act}, and noise is added to the measured output after anti-aliasing filters. ΔG and W_{in} represent the multiplicative uncertainty and its weighting function respectively. The transfer function ΔG is assumed to be stable and unknown, except for being uniformly distributed within the norm-bounded set of $\|\Delta G\|_\infty \leq 1$. Note that this uncertainty description cannot be represented by uncertainty matrix Δ in (2.2); however, the estimation of γ_{ij} can still be estimated by generating random samples of ΔG, and the reliability analysis follows identical procedures.

By incorporating performance weighting functions, W_{act}, W_n, W_p, and W_β, a generalized plant with 26th order can be constructed from Figure 2.3, corresponding to the nominal fault-free regime model $\mathcal{M}(\zeta(t),\ \eta(t))$ in (2.2) for $\zeta(t) = \eta(t) = 0$. The control objectives

are converted to closed-loop $\mathcal{H}_\infty$ norm, $\|G_{zw}(\zeta(t), \eta(t), s)\|_\infty$, where w is the vector of lateral stick and rudder pedal, and $z = [e_p^T \; e_\beta^T \; e_{\text{act}}^T]^T$. An $\mathcal{H}_\infty$ controller $K_0(s)$ is designed for the nominal fault-free model, which achieves $\mathcal{H}_\infty$ norm of 0.6671. For brevity, the parameters of the generalized plant and controller are not given here. See [47] for the details of design procedure.

Consider two fault scenarios that the effectiveness of two actuators are reduced by half respectively, denoted by $B_{\text{F14}}^{\text{f1}} = B_{\text{F14}} \begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix}$ and $B_{\text{F14}}^{\text{f2}} = B_{\text{F14}} \begin{bmatrix} 1 & 0 \\ 0 & 0.5 \end{bmatrix}$, where $B_{\text{F14}}^{\text{f1}}$ and $B_{\text{F14}}^{\text{f2}}$ denote the values of B_{F14} under faults.

Following similar procedure as the fault-free mode, the generalized plants under faults can be derived, corresponding to the faulty regime models in (2.2). And other two controllers, $K_1(s)$ and $K_2(s)$, are designed accordingly for the plant under two actuator faults respectively, which achieve $\mathcal{H}_\infty$ norms of 1.0558 and 0.7021 respectively.

The performance evaluation function is defined as

$$J(\zeta(t),\, \eta(t)) = \mu(\mathcal{M}(\zeta(t),\, \eta(t)) = \begin{cases} 1, \text{ internally unstable at } t, \\ \frac{\|G_{zw}(\zeta(t),\eta(t),s)\|_\infty}{1+\|G_{zw}(\zeta(t),\eta(t),s)\|_\infty}, \text{ internally stable at } t, \end{cases}$$

and $J_{\text{max}}^0 = 0.5455$, $J_{\text{max}}^1 = J_{\text{max}}^2 = 0.6000$. Note that performance degradation has been considered since J_{max}^1 and J_{max}^2 are greater than J_{max}^0. The hard deadline T_{hd} is assumed to be 1 minute.

$\zeta(t)$ and $\eta(t)$ are taking values from $S_1 = S_2 = \{0,\ 1,\ 2\}$ in which the three modes denote fault-free mode and the loss of effectiveness in the first and second actuator respectively. The generator matrices of these Markov processes are given as follows to describe fault occurrences and FDI results:

$$H_\zeta = \begin{bmatrix} -0.003 & 0.001 & 0.002 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ H_\eta^0 = \begin{bmatrix} -0.02 & 0.01 & 0.01 \\ 2 & -2.01 & 0.01 \\ 2 & 0.01 & -2.01 \end{bmatrix},$$

$$H_\eta^1 = \begin{bmatrix} -2.01 & 2 & 0.01 \\ 0.01 & -0.02 & 0.01 \\ 0.01 & 2 & -2.01 \end{bmatrix},\ H_\eta^2 = \begin{bmatrix} -2.01 & 0.01 & 2 \\ 0.01 & -2.01 & 2 \\ 0.01 & 0.01 & -0.02 \end{bmatrix}.$$

The time unit of transition rates is selected as minute. According to H_ζ, the mean occurrence time is 1000 minutes for the first fault mode and 500 minutes for the second fault, and both fault modes are absorbing. For FDI modes, according to the first row of H_η^0, when the aircraft is in fault-free mode, the mean time of false alarms is 100 minutes; and according to its second row, the mean time to return to correct detection after a false alarm is 0.5 minutes. H_η^1 and H_η^2 can be interpreted similarly.

Following the definitions given in Section 2.4.2, four probabilistic parameters are calculated as follows:

$$\gamma \triangleq \begin{bmatrix} \gamma_{00} & \gamma_{01} & \gamma_{02} \\ \gamma_{10} & \gamma_{11} & \gamma_{12} \\ \gamma_{20} & \gamma_{21} & \gamma_{22} \end{bmatrix} = \begin{bmatrix} 0.8600 & 0 & 0 \\ 0 & 0.7000 & 0 \\ 0 & 0 & 0.9600 \end{bmatrix},$$

$$\pi \triangleq \begin{bmatrix} \pi_0^0 & \pi_1^0 & \pi_2^0 \\ \pi_0^1 & \pi_1^1 & \pi_2^1 \\ \pi_0^2 & \pi_1^2 & \pi_2^2 \end{bmatrix} = \begin{bmatrix} 0.9901 & 0.0050 & 0.0050 \\ 0.0050 & 0.9901 & 0.0050 \\ 0.0050 & 0.0050 & 0.9901 \end{bmatrix},$$

$$w \triangleq \begin{bmatrix} w_0^0 & w_1^0 & w_2^0 \\ w_0^1 & w_1^1 & w_2^1 \\ w_0^2 & w_1^2 & w_2^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; v \triangleq \begin{bmatrix} v_0^0 & v_1^0 & v_2^0 \\ v_0^1 & v_1^1 & v_2^1 \\ v_0^2 & v_1^2 & v_2^2 \end{bmatrix} = \begin{bmatrix} 0.9333 & 0.0333 & 0.0333 \\ 0.0161 & 0.9677 & 0.0161 \\ 0.1000 & 0.1000 & 0.8000 \end{bmatrix}.$$

γ is calculated based on the closed-loop plant regime models of this F-14 aircraft and $\mathcal{H}_\infty$ norm objective by using a randomized algorithm and taking the random samples of ΔG within its bounded set (Tempo *et al.*, 1998). According to γ, the probability of satisfying the bounds of $\mathcal{H}_\infty$ norm under each mode is 0.86, 0.7, and 0.9 respectively if FDI gives correct detection. According to π, the stationary probability of correct detection is 0.9901. According to w, when the bounds of $\mathcal{H}_\infty$ norm are satisfied, the probability that the FDI gives correct detection are 1, but FDI may have given wrong estimates of fault modes when the bounds of $\mathcal{H}_\infty$ norm are not satisfied according to v.

The state space of $X^{\mathrm{R}}(t)$ contains 7 states for this system: $S_{\mathrm{r}} = \{0_{\mathrm{N}}, 0_{\mathrm{F}}, 1_{\mathrm{N}}, 1_{\mathrm{F}}, 2_{\mathrm{N}}, 2_{\mathrm{F}}, \mathrm{F}\}$. With the above probabilistic parameters calculated from the F-14 aircraft model, the semi-Markov kernel of $X^{\mathrm{R}}(t)$ for reliability evaluation is obtained by following the procedure in Section 2.4.3. The transition probabilities and reliability curve are then calculated as shown in Figure 2.4. Each transition probability curve in Figure 2.4 gives the probability that $X^{\mathrm{R}}(t)$ is in each state at t starting from the initial state 0_{N}. From the curves of reliability and the transition probability to state F, it is clear that system failure probability remains at 0 within T_{hd}, a finding consistent with our reliability definition as temporal violation of control objectives is not deemed as a failure. We also find $P(0_{\mathrm{N}}, 2_{\mathrm{N}}, t)$ is much larger than $P(0_{\mathrm{N}}, 1_{\mathrm{N}}, t)$, a finding consistent with $H_\zeta(1,3) > H_\zeta(1,2)$ and $\gamma_{22} > \gamma_{11}$.

According to Figure 2.4, the probability of transiting to state 0_{F} is much higher than those to 1_{F} and 2_{F}. So $X^{\mathrm{R}}(t)$ transits to F mainly from 0_{F}. This implies that the false alarm of FDI at the fault-free mode is more likely the reason for system failure than fault occurrences themselves, a finding useful for system reliability improvement. To verify this finding, the false alarm rates for $\zeta(t) = 0$ is reduced by half by setting $H_\eta^0(1,2) = H_\eta^0(1,3) = 0.005$ and $H_\eta^0(1,1) = -0.01$. The transition probability and reliability curves for the system after reducing false alarms are shown in Figure 2.5. As we expected, $P(0_{\mathrm{N}}, 0_{\mathrm{F}}, t)$

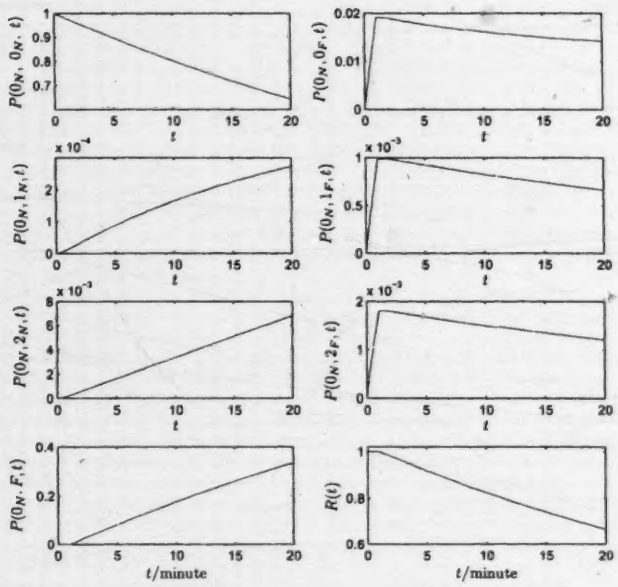

Figure 2.4: Transition probability and reliability function.

is reduced, and $R(t)$ is improved. We may also calculate and compare the MTTF of both cases: the MTTF of the system before reducing FDI false alarms is 47.3415 minutes while the MTTF after reducing false alarms is 80.9144 minutes.

On the other hand, the sensitivity of reliability index with respect to control performance can also be demonstrated. Let probabilistic parameters be improved to $\gamma_{00} = \gamma_{11} = \gamma_{22} = 0.99$. Based on the definitions of i_N in (5.4) and γ_{ij} in (2.4), we expect increases in transition probabilities to i_N, $i \in S_1$. The transition probability and reliability curves for FTCS's with improved control performance are shown in Figure 2.6. Compared with Figure 2.4, $P(0_N,\ 0_N,\ t)$, $P(0_N,\ 1_N,\ t)$, and $P(0_N,\ 2_N,\ t)$ are clearly improved. As a result, the reliability curve is also improved and MTTF increases to 76.7722 minutes compared to the original MTTF of 47.3415 minutes. So the transition probability of $X^R(t)$ can not only give reliability evaluation but also help to find out the effective solution to improve reliability.

2.6 Conclusions

A reliability evaluation approach for active FTCS's is presented in this chapter. The index reflects the characteristics of FTCS's, including a model-based control performance

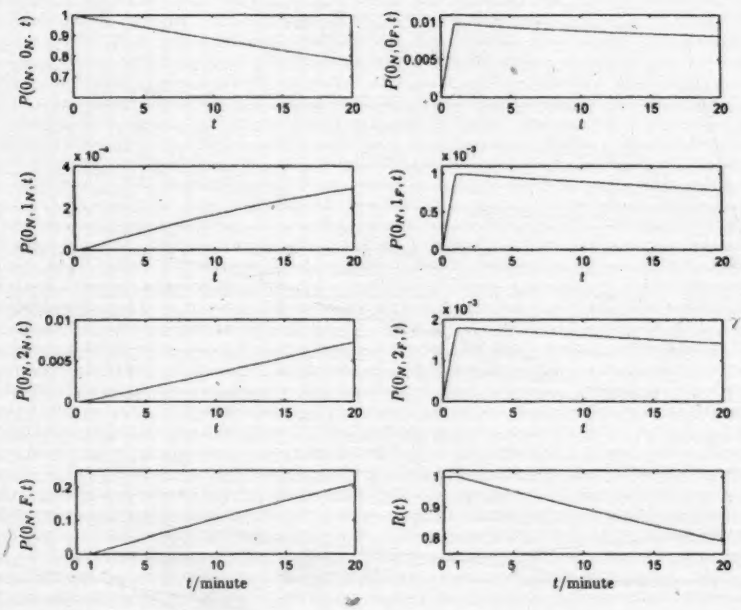

Figure 2.5: Transition probability and reliability function with improved FDI scheme.

and hard deadline concept. The semi-Markov model is constructed based four probabilistic parameters, and reliability can be thereby calculated. The transition probabilities and reliability function provide valuable information on the long-term safety behavior of FTCS's. Moreover, the effects of FDI and control performance on reliability are demonstrated in an illustrative example. With this reliability index and modeling method available, reliability-based controller can be designed to optimize overall system reliability.

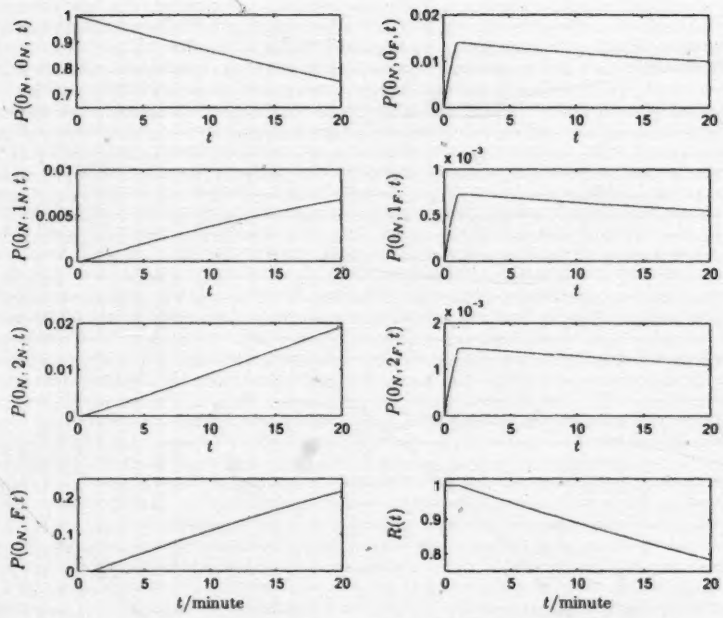

Figure 2.6: Transition probability and reliability function with improved controller.

Chapter 3

Probabilistic controller design via stabilizing controller parameterization*

3.1 Introduction

This chapter addresses the design of FTCS's in the following configuration: Consider a plant with a finite set of fault modes S_1, and $\mathbf{G} = \{G_i : i \in S_1\}$ represents the set of dynamical plant models under various fault modes. The evolution of these modes can be represented by a Markov process. Usually fault mode is not directly known to controller, and an FDI scheme is used to generate estimates from a finite set S_2. But FDI modes may deviate from true fault modes with an error probability, so another Markov process is adopted to represent FDI modes. The reconfigurable controller denoted by $\mathbf{K} = \{K_j : j \in S_2\}$ is assumed to have a switching structure, and K_j is engaged for the plant when the FDI is in mode j.

This stochastic FTC model is preferable to deterministic ones when considering a probabilistic performance criterion. In contrast to the assumption of known regime or fault modes in regular Jump Linear Systems (JLS's), this model assumes unknown fault modes and uses an additional Markov process to represent its estimate, the FDI mode. If FDI scheme gives a wrong detection mode j, K_j may be used for plant model G_i, $i \neq j$, even though K_j is originally designed for G_j. As a result of this difference, the design of FTCS's is more challenging, and many existing methods for JLS's cannot be directly applied, e.g., [51, 52, 53, 54]. The related problem in JLS's to this FTC configuration is the partial observation problem [55], which used conditional probability as the estimation precision

*Originally published as: Hongbin Li and Qing Zhao, " Probabilistic Design of Fault Tolerant Control via Parameterization", *Circuits, Systems, and Signal Processing*, vol. 26, no. 3, pp. 325-351, 2007.

of regime modes but estimation delay cannot be described. In the literature of FTCS's, Mariton studied the effects of this FDI imperfection including detection delay on system stability [6]; Srichander and Walker developed the conditions for exponential mean-square stability [15]; and much of the latest work was also based on this model, such as output feedback stabilization [56], H_2 control [57], and the H_∞ control of a sampled-data system [58]. However, these results considered control objectives only, and system reliability index was not discussed.

In our problem, in addition to stability requirement, another design objective $\psi(\mathbf{K})$ of closed-loop system is evaluated for each controller $\mathbf{K}$ via a numerical method. The design goal is to find the optimal controller $\mathbf{K}^*$ that can optimize $\psi(\mathbf{K})$ subject to stability constraint. The motivation is to design FTCS's based on the reliability index presented in Chapter 2, which is evaluated based on a semi-Markov model. Owing to the numerical procedures of building and solving stochastic reliability models, reliability criteria cannot be written as analytical functions of $\mathbf{K}$ in general. To overcome this difficulty, stabilizing controller parameterization and randomization-based optimization algorithms are proposed for FTCS's in this chapter to find the statistically optimal controller with the highest reliability.

Controller parameterization plays an important role in systems and control theory, which can facilitate the design of optimal controller by using Linear Matrix Inequalities (LMI's) or other classical optimization techniques. For linear systems, many parameterization results have been reported, such as Youla parameterization [59], $\mathcal{H}_\infty$ controller parameterization by Riccati equations and by LMI's [60, 61, 62], covariance controller parameterization [63, 64], and stabilizing controller parameterization using quadratic Lyapunov functions [65]. However, to the best of authors' knowledge, no controller parameterization result has been reported for FTCS's.

Classical optimization techniques and LMI methods usually require objective function $\psi(\cdot)$ and parameterization expression to be affine with respect to free parameters [66]. However, in our problem, even the analytical expression of $\psi(\cdot)$ is not available, and a numerical method has to be used to calculate $\psi(\cdot)$. In this case, some statistical methods, such as the randomized algorithms, are useful to perform the design [67, 46, 54].

To recapitulate, this chapter presents a parameterization result of stabilizing controllers for stochastic FTCS's and a randomization-based optimization method to search for the statistically optimal controller with respect to a numerical design objective, e.g., a reliability criterion. The remainder of this chapter is organized as follows: Section 3.2 states system model and problem formulation; Section 3.3 provides some mathematical preliminar-

ies; Sections 3.4 through 3.7 present the main results: stabilization conditions, controller parameterization, the analysis of stabilizing controller set, and the synthesis of generator matrices; and an example is given in Section 3.8 followed by conclusions in Section 3.9.

3.2 Problem formulation

The general Markov dynamical model of FTCS's is given by 2.2 in Chapter 2. When considering internal stability, it can be reduced to the following equation by removing exogenous input and output equations:

$$\dot{x}(t) = A(\zeta(t), \Delta)x(t) + B(\zeta(t), \Delta)u(\eta(t), t), \tag{3.1}$$

where $x(t) \in \mathbb{R}^n$ and $u(\eta(t), t) \in \mathbb{R}^m$ denote system state and control input respectively, and $A(\zeta(t), \Delta)$ and $B(\zeta(t), \Delta)$ system matrices with appropriate dimensions. (3.1) represent a set of linear dynamical models $\mathbf{G} = \{G_i : i \in S_1\}$, where G_i denotes the dynamical model when $\zeta(t) = i$. $\zeta(t)$ and $\eta(t)$ are assumed to be two separate continuous-time Markov processes with finite state spaces $S_1 = \{0, 1, 2, \cdots, N_1\}$ and $S_2 = \{0, 1, 2, \cdots, N_2\}$ to represent system faults and FDI results respectively. Detailed descriptions have been provided in Chapter 2 and are omitted here for brevity.

The closed-loop system structure is shown in Figure 3.1. Here we consider static state-feedback controller, $u(\eta(t), t) = K(\eta(t))x(t)$. For simplicity, we write $u_j(t) = K_j x(t)$ for $\eta(t) = j \in S_2$. The controller is composed of a set of static gains, denoted by $\mathbf{K} = \{K_0, K_1, \cdots, K_{N_2}\}$. When $\eta(t)$ indicates fault mode i, K_i is in use. In practice, it is impossible to have a "perfect" FDI that always instantaneously indicates the correct fault mode. Hence, there may be mismatch between $\eta(t)$ and $\zeta(t)$. In this case, finding $\mathbf{K}$ to achieve nominal closed-loop stability (when $\Delta = 0$) is the first concern in the design of FTCS's.

Remark 3.1 *The interaction between $\zeta(t)$ and $\eta(t)$ causes the major difficulty in the stabilizing design of FTCS's. This is the main difference between FTCS's and regular JLS's.*

Such a stabilizing controller $\mathbf{K}$ is usually not unique. In fact, the set of all stabilizing controllers can be found via parameterization. When considering a more specific performance criterion $\psi(\mathbf{K})$, it is desirable to obtain the optimal stabilizing controller $\mathbf{K}^*$ with respect to $\psi(\mathbf{K})$. This leads to the second stage of design. In this chapter, such a $\psi(\mathbf{K})$ is chosen as a reliability criterion.

A stochastic process model is constructed in Chapter 2 to describe the evolution of control performance under fault occurrences and controller reconfigurations. $R(t)$ and MTTF

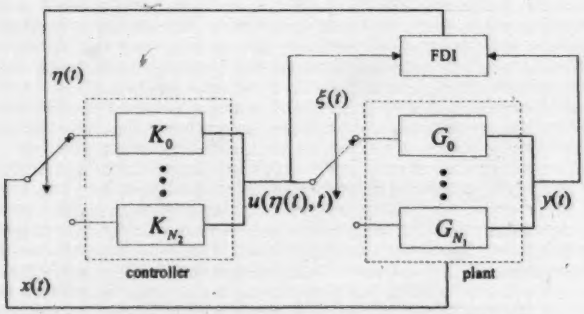

Figure 3.1: The system structure.

can be calculated based on the transition and stationary probabilities of the stochastic process. However, neither of these two reliability criteria has analytic function expressions available. In this chapter, $\psi(\mathbf{K})$ is selected as the scalar reliability index, MTTF.

Based on such a $\psi(\mathbf{K})$, a randomization procedure is available to find a statistical optimum $\hat{\mathbf{K}}^*$, an estimate of $\mathbf{K}^*$, such that

$$\Pr\{\Pr\{\psi(\mathbf{K}^*) > \psi(\hat{\mathbf{K}}^*)\} \leq \epsilon\} \geq 1 - \delta, \tag{3.2}$$

where $\epsilon \in (0,1)$ and $\delta \in (0,1)$ are precision parameters of the estimate.

The main procedure of the randomized algorithm presented in [46] is summarized as follows, where the key step is to find a parameterization set of stabilizing controllers: $\mathcal{K} \triangleq \{\text{All stabilizing } \mathbf{K}\} = \{\mathbf{K} | \mathbf{K} = \varphi(z),\ z \in \Omega\}$, where $\varphi : \Omega \to \mathcal{K}$ denotes the parameterization mapping from a free parameter z within a bounded set Ω to a stabilizing controller $\mathbf{K}$.

Algorithm 3.1 - estimate the statistical optimum

1) Determine sample quantity $M_1 \geq \frac{1/\delta}{1/(1-\epsilon)}$ based on the precision parameters ϵ and δ [46].

2) Generate M_1 independent samples $z^{(1)}, \cdots, z^{(M_1)}$ in Ω according to the distribution of z. Calculate the corresponding controllers $\mathbf{K}^{(i)} = \varphi(z^{(i)}), i = 1, \cdots, M_1$.

3) Evaluate the performance value at each sample controller $\mathbf{K}^{(i)}$:

$$\psi_i = \psi(\mathbf{K}^{(i)}) = \psi(\varphi(z^{(i)})),\ i = 1, \cdots M_1.$$

Let z_0 denote the parameter such that $\psi(\varphi(z_0)) = \max_{1 \leq i \leq M_1} \psi_i$. Then $\hat{\mathbf{K}}^* = \varphi(z_0)$.

The remainder is then focused on developing a parameterization method for Algorithm 3.1.

3.3 Preliminaries

The following notation is used throughout the chapter: A^{-T} means $(A^T)^{-1}$. $A^\perp$ denotes a matrix with the following properties: $\mathcal{N}(A^\perp) = \mathcal{R}(A)$ and $A^\perp A^{\perp T} > 0$, where $\mathcal{N}(A)$ and $\mathcal{R}(A)$ denote the null and range spaces of A respectively. $\triangleq$ is used for notation definitions. $\|\cdot\|$ denotes the Euclidean norm for vectors and the largest singular value for matrices. $\mathbb{R}$ denotes the set of real numbers, and $\mathbb{N}$ the set of nonnegative integers. For notational simplicity, in (3.1), for $\zeta(t) = i$, $\eta(t) = j$, $i \in S_1$, $j \in S_2$, denote $A_i \triangleq A(\zeta(t))$, $B_i \triangleq B(\zeta(t))$, and $u_j(t) \triangleq u(\eta(t), t)$.

Definition 3.1 (EMS stability [15]) *An FTCS is said to be Exponentially Mean-Square (EMS) stable if for any initial Markov states at $t = 0$, $\zeta(0)$ and $\eta(0)$, there exist $a > 0$, $b > 0$, and some number $\delta(\zeta(0), \eta(0)) > 0$, such that when $\|x(0)\| \leq \delta(\zeta(0), \eta(0))$, the following inequality holds for $t \geq 0$:*

$$E\{\|x(t)\|^2\} \leq b\|x(0)\|^2 e^{-at},$$

where $E\{\cdot\}$ denotes the mathematical expectation.

Lemma 3.1 (Stability conditions [15]) *An FTCS in (3.1) is stabilized in the sense of EMS stability by the static state-feedback control law*

$$u_i(t) = K_i x(t),\ i \in S_2,$$

if and only if for any given $k \in S_1$ and $i \in S_2$, there exist positive-definite matrices $P_{ik} > 0$, satisfying

$$\tilde{A}_{ik}^T P_{ik} + P_{ik}\tilde{A}_{ik} + \sum_{j \in S_2, j \neq i} \beta_{ij}^k P_{jk} + \sum_{j \in S_1, j \neq k} \alpha_{kj} P_{ij} < 0,$$

where

$$\tilde{A}_{ik} \triangleq A_k + B_k K_i - 0.5 \sum_{j \in S_2, j \neq i} \beta_{ij}^k - 0.5 \sum_{j \in S_1, j \neq k} \alpha_{kj}.$$

Lemma 3.1 can be used for stability analysis for a given state-feedback controller, but it is difficult to solve K_i directly using these inequalities. The main difficulty lies in the fact that the number of gains K_i is less than that of inequalities involved in the above condition such that each K_i should satisfy multiple inequalities simultaneously. In contrast, regular JLS's do not have this problem, and the controller can be solved using LMI's [52]. The partial observation problem of JLS considered in [68] has similar form as in FTCS's but only a sufficient condition was derived. See [69, 57] for more discussions.

The following two lemmas are introduced for the purpose of deriving stabilization conditions and a parameterization set.

Lemma 3.2 (Finsler's theorem [62, 64]) *Let matrices $M \in \mathbb{R}^{n\times m}$ and $Q \in \mathbb{R}^{n\times n}$ be given, and assume that* $\mathrm{rank}(M) < n$ *and $Q = Q^T$. Let (M_L, M_R) be any full rank factors of M such that $M = M_L M_R$ and* $\mathrm{rank}(M_L) = \mathrm{rank}(M_R) = \mathrm{rank}(M)$. *Then*

$$M^{\perp} Q M^{\perp T} < 0$$

if and only if

$$\mu M M^T - Q > 0$$

for some $\mu \in \mathbb{R}$. If the above condition holds, all such μ are given by

$$\mu > \mu_{\min} \triangleq \lambda_{\max}[N(Q - QM^{\perp T}(M^{\perp} Q M^{\perp T})^{-1} M^{\perp} Q) N^T],$$

where $\lambda_{\max}(\cdot)$ denotes the largest eigenvalue, and $N \triangleq (M_R M_R^T)^{(-1/2)}$.

Lemma 3.3 (Projection lemma and parameterization set) *Let matrices $M \in \mathbb{R}^{n\times m}$, and $Q = Q^T \in \mathbb{R}^{n\times n}$ be given. The following two statements are equivalent:*

1) There exists a matrix X satisfying

$$MX + (MX)^T + Q < 0. \tag{3.3}$$

2) The following condition holds:

$$M^{\perp} Q M^{\perp T} < 0 \text{ or } M M^T > 0. \tag{3.4}$$

If statement 2) holds, all matrices X satisfying statement 1) are given by

$$X = g(L, \rho | M, Q) \triangleq -\rho^{-1} M^T + \rho^{-1/2} L (\rho^{-1} M M^T - Q)^{1/2}, \tag{3.5}$$

where L is an arbitrary matrix satisfying $\|L\| < 1$, and $\rho \in (0,\ \rho_{\max})$ a positive scalar. L and ρ are immediate variables of function g, and the symbol '$|$' in (3.5) is used to indicate the dependence of X on M and Q.

$\rho_{\max} = a^{-1}$ is calculated by solving the following LMI problem:

$$\mathrm{Min}_{\{a,X\}} a$$

subject to

$$\begin{aligned} a &> 0, \\ \begin{bmatrix} -aI & X \\ X^T & MX + (MX)^T + Q \end{bmatrix} &< 0. \end{aligned} \tag{3.6}$$

Moreover, $\rho \in (0,\ \rho_{\max})$ *if and only if it satisfies*

$$\rho^{-1} M M^T - Q > 0, \tag{3.7}$$

which ensures that $(\rho^{-1} M M^T - Q)^{1/2}$ *exists and that (3.5) is valid.*

Proof: The equivalence between statements 1) and 2) is a special form of the well-known Projection Lemma [66]. Here, we prove (3.5) only. When the statements 1) and 2) hold, it is equivalent to

$$MX + (MX)^T + \rho X^T X < -Q, \tag{3.8}$$

for some scalar $\rho > 0$. Add $\rho^{-1} M M^T$ to both sides, complete the square in the left hand side of (3.8), and we have

$$(\rho^{-1} M + X^T)\rho(\rho^{-1} M^T + X) < \rho^{-1} M M^T - Q. \tag{3.9}$$

Obviously, (3.9) holds if and only if $\rho^{-1} M M^T - Q > 0$ as the left hand side of (3.9) is positive semi-definite. By taking the matrix square root, (3.9) is equivalent to

$$(\rho^{-1} M M^T - Q)^{-1/2}(M\rho^{-1} + X^T)\rho(\rho^{-1} M^T + X)(\rho^{-1} M M^T - Q)^{-1/2} < I. \tag{3.10}$$

Define $L \triangleq \rho^{1/2}(\rho^{-1} M^T + X)(\rho^{-1} M M^T - Q)^{-1/2}$. Then $\|L\| < 1$ and

$$X = -\rho^{-1} M^T + \rho^{-1/2} L (\rho^{-1} M M^T - Q)^{1/2}.$$

To determine the upper bound of ρ, convert (3.8) to the following matrix inequality by Schur's complement lemma [66]:

$$\begin{bmatrix} -\rho^{-1} I & X \\ X^T & MX + (MX)^T + Q \end{bmatrix} < 0.$$

Define a new decision variable $a \triangleq \rho^{-1} > 0$, and the minimum value of a gives the upper bound $\rho_{\max}$. Moreover, $\rho \in (0,\ \rho_{\max})$ ensures $\rho^{-1} M M^T - Q > 0$ owing to (3.9). ■

Lemma 3.3 is adopted from Corollary 2.3.9 in [64] with modifications to make it suitable for our problem. For a given inequality in the form of (3.3), Lemma 3.3 provides a solvability condition and a parameterization set of all its solutions:

$$\mathcal{G}_{M,Q} = \{X | X = g(L, \rho | M, Q),\ \|L\| < 1,\ \rho \in (0, \rho_{\max})\}, \tag{3.11}$$

where $g(L, \rho | M, Q)$ is defined in (3.5).

3.4 Stabilization conditions

Let us begin with the case that the state spaces of $\zeta(t)$ and $\eta(t)$, S_1 and S_2, are both equal to $\{0, 1\}$, where '0' denotes the fault-free situation and '1' the faulty mode. This type of FTCS's is referred to as the basic case. The stochastic behavior of $\zeta(t)$ is governed by its generator matrix F; when $\zeta(t) = 0$ or 1, the behavior of $\eta(t)$ is determined by the corresponding generator matrix H^0 or H^1 [25, 70].

The generator matrices are composed of the transition rates of $\zeta(t)$ and $\eta(t)$, α_{ij} and β_{ij}^k, which have the following forms for the basic case:

$$H_\zeta = \begin{bmatrix} -\alpha_{00} & \alpha_{01} \\ \alpha_{10} & -\alpha_{11} \end{bmatrix}, \; H_\eta^0 = \begin{bmatrix} -\beta_{00}^0 & \beta_{01}^0 \\ \beta_{10}^0 & -\beta_{11}^0 \end{bmatrix}, \; H_\eta^1 = \begin{bmatrix} -\beta_{00}^1 & \beta_{01}^1 \\ \beta_{10}^1 & -\beta_{11}^1 \end{bmatrix}.$$

For the system in (3.1), by Lemma 3.1, $\{K_0, K_1\}$ stabilizes the FTCS's in the sense of EMS stability if and only if there exist positive definite matrices $P_{ik}, i \in S_2, k \in S_1$, such that the following inequalities hold simultaneously:

$$P_{00}B_0K_0 + (P_{00}B_0K_0)^T + Q_{00} < 0, \tag{3.12}$$

$$P_{10}B_0K_1 + (P_{10}B_0K_1)^T + Q_{10} < 0, \tag{3.13}$$

$$P_{01}B_1K_0 + (P_{01}B_1K_0)^T + Q_{01} < 0, \tag{3.14}$$

$$P_{11}B_1K_1 + (P_{11}B_1K_1)^T + Q_{11} < 0, \tag{3.15}$$

where $Q_{ik}, i \in S_2, k \in S_1$, is defined as

$$Q_{ik} \triangleq (A_k - 0.5\beta_{i(1-i)}^k - 0.5\alpha_{k(1-k)})^T P_{ik} + P_{ik}(A_k - 0.5\beta_{i(1-i)}^k$$

$$-0.5\alpha_{k(1-k)}) + \beta_{(1-i)k}^k P_{i(1-k)} + \alpha_{k(1-k)} P_{i(1-k)}. \tag{3.16}$$

The set of all stabilizing controllers can be captured naturally by posing a matrix inequality problem (3.12)-(3.15) for $\{K_0, K_1\}$. Note that both K_0 and K_1 appear in two inequalities. So the intersection of the solution sets of (3.12) and (3.14) gives the set of K_0, and K_1 can be obtained in a similar way from (3.13) and (3.15).

Lemma 3.4 *For the basic case of FTCS's in (3.1), if B_0 and B_1 are row rank deficient, then there exists a stabilizing state-feedback controller $\{K_0, K_1\}$ in the sense of EMS stability only if there exist positive-definite matrices P_{ik}, $k \in S_1 = \{0, 1\}$, $i \in S_2 = \{0, 1\}$, such*

that

$$(P_{00}B_0)^{\perp}Q_{00}(P_{00}B_0)^{\perp T} < 0, \tag{3.17}$$

$$(P_{10}B_0)^{\perp}Q_{10}(P_{10}B_0)^{\perp T} < 0, \tag{3.18}$$

$$(P_{01}B_1)^{\perp}Q_{01}(P_{01}B_1)^{\perp T} < 0, \tag{3.19}$$

$$(P_{11}B_1)^{\perp}Q_{11}(P_{11}B_1)^{\perp T} < 0, \tag{3.20}$$

where Q_{ik} is defined in (3.16). If B_0 has full row rank, (3.17) and (3.18) are removed from the conditions; if B_1 has full row rank, (3.19) and (3.20) are removed.

Proof: Based on Lemma 3.3, each inequality in (3.12)-(3.15) has feasible solution K_0 or K_1 if and only if the the corresponding condition in (3.17)-(3.20) holds. Considering that (3.12)-(3.15) must hold simultaneously for system stability, (3.17)-(3.20) are only necessary conditions. If B_0 has full row rank, (3.12) and (3.13) always have feasible solutions for any P_{00}, P_{10}, Q_{00} and Q_{10}, so (3.17) and (3.18) are removed; similarly, if B_1 has full row rank, (3.19) and (3.20) are removed. ■

This lemma is derived based on Lemma 3.1, and the proof is given in the appendix. By converting the inequalities in Lemma 3.4 to LMI's, we have the following theorem.

Theorem 3.1 *For the basic case of FTCS's in (3.1), if B_0 and B_1 are row rank deficient, and all the transition rates of $\zeta(t)$ and $\eta(t)$ are nonzero, then there exist stabilizing state-feedback controllers in the sense of EMS stability only if there exist positive-definite matrices P_{ik}, positive scalars μ_{ik}, $k \in S_1 = \{0,1\}$, $i \in S_2 = \{0,1\}$, such that*

$$\begin{bmatrix} P_{00}^{-1}\bar{A}_{00}^T + \bar{A}_{00}P_{00}^{-1} - \mu_{00}B_0B_0^T & P_{00}^{-1} & P_{00}^{-1} \\ P_{00}^{-1} & -P_{10}^{-1}/\beta_{01}^0 & 0 \\ P_{00}^{-1} & 0 & -P_{01}^{-1}/\alpha_{01} \end{bmatrix} < 0, \tag{3.21}$$

$$\begin{bmatrix} P_{10}^{-1}\bar{A}_{10}^T + \bar{A}_{10}P_{10}^{-1} - \mu_{10}B_0B_0^T & P_{10}^{-1} & P_{10}^{-1} \\ P_{10}^{-1} & -P_{00}^{-1}/\beta_{10}^0 & 0 \\ P_{10}^{-1} & 0 & -P_{11}^{-1}/\alpha_{01} \end{bmatrix} < 0, \tag{3.22}$$

$$\begin{bmatrix} P_{01}^{-1}\bar{A}_{01}^T + \bar{A}_{01}P_{01}^{-1} - \mu_{01}B_1B_1^T & P_{01}^{-1} & P_{01}^{-1} \\ P_{01}^{-1} & -P_{11}^{-1}/\beta_{01}^1 & 0 \\ P_{01}^{-1} & 0 & -P_{00}^{-1}/\alpha_{10} \end{bmatrix} < 0, \tag{3.23}$$

$$\begin{bmatrix} P_{11}^{-1}\bar{A}_{11}^T + \bar{A}_{11}P_{11}^{-1} - \mu_{11}B_1B_1^T & P_{11}^{-1} & P_{11}^{-1} \\ P_{11}^{-1} & -P_{01}^{-1}/\beta_{10}^1 & 0 \\ P_{11}^{-1} & 0 & -P_{10}^{-1}/\alpha_{10} \end{bmatrix} < 0, \tag{3.24}$$

where $\bar{A}_{ik} \triangleq A_k - 0.5\beta_{i(1-i)}^k - 0.5\alpha_{k(1-k)}$. In case that B_0 has full row rank, (3.21) and (3.22) are removed from the conditions; if B_1 has full row rank, (3.23) and (3.24) are

removed. If some transition rates are zero, the corresponding rows and columns containing those zero transition rates are removed from the above matrices.

Proof: Take (3.17) as an example, and the derivations are similar for the other three inequalities. As $P_{00} > 0$ and $(P_{00}B_0)^{\perp}((P_{00}B_0)^{\perp})^T > 0$, both $(P_{00}B_0)^{\perp}$ and $(P_{00}B_0)^{\perp}P_{00}$ have full row rank. Considering $(P_{00}B_0)^{\perp}P_{00}B_0 = 0$ and $(P_{00}B_0)^{\perp}P_{00} = B_0^{\perp}$, we have

$$(P_{00}B_0)^{\perp} = B_0^{\perp}P_{00}^{-1}.$$

So (3.17) is equivalent to

$$B_0^{\perp}P_{00}^{-1}Q_{00}P_{00}^{-1}B_0^{\perp T} < 0.$$

Substitute Q_{00} and denote $\bar{A}_{00} \triangleq A_0 - 0.5\beta_{01}^0 - 0.5\alpha_{01}$ to obtain

$$B_0^{\perp}(P_{00}^{-1}\bar{A}_{00}^T + \bar{A}_{00}P_{00}^{-1} + \beta_{01}^0 P_{00}^{-1}P_{10}P_{00}^{-1} + \alpha_{01}P_{00}^{-1}P_{01}P_{00}^{-1})B_0^{\perp T} < 0.$$

By Lemma 3.2, this inequality is equivalent to

$$P_{00}^{-1}\bar{A}_{00}^T + \bar{A}_{00}P_{00}^{-1} + \beta_{01}^0 P_{00}^{-1}P_{10}P_{00}^{-1} + \alpha_{01}P_{00}^{-1}P_{01}P_{00}^{-1} < \mu_{00}B_0B_0^T, \tag{3.25}$$

where $\mu_{00} \in \mathbb{R}$. Pre- and post-multiply P_{00},

$$\bar{A}_{00}^T P_{00} + P_{00}\bar{A}_{00} + \beta_{01}^0 P_{10} + \alpha_{01}P_{01} < \mu_{00}P_{00}B_0B_0^T P_{00}. \tag{3.26}$$

According to Lemma 3.2, all feasible μ_{00} are given by $\mu_{00} > \mu_{00\min}$, where $\mu_{00\min}$ can be calculated by the parameters in the inequality. Therefore, if the feasible set of μ_{00} is non-empty, there must be a feasible $\mu_{00} > 0$. Furthermore, we need to consider only the positive case of μ_{00} to obtain all the feasible P_{ij} owing to the following reasoning:

Suppose for any two feasible values of μ_{00}, $\mu_1 \leq 0$ and $\mu_2 > 0$, all the corresponding feasible solutions of P_{ij} in (3.25), $i, j \in \{0, 1\}$, are denoted by $\mathcal{P}_1$ and $\mathcal{P}_2$. For every element $P_{ij} \in \mathcal{P}_1, i, j \in \{0, 1\}$, (3.25) holds for this P_{ij} and μ_1. Again, based on Lemma 3.2, this element $P_{ij}, i, j \in \{0, 1\}$, is also feasible for (3.25) corresponding to μ_2 as $\mu_2 > \mu_1$ and thereby belongs to $\mathcal{P}_2$. Therefore, $\mathcal{P}_1 \subseteq \mathcal{P}_2$, which means that the feasible solution of $P_{ij}, i, j \in \{0, 1\}$, for (3.25) when $\mu \leq 0$ is a subset of those when $\mu > 0$, and we need to consider this positive case only.

Suppose that the transition rates $\beta_{01}^0 > 0$ and $\alpha_{01} > 0$. By Schur's complement lemma [66], (3.25) is equivalent to

$$\begin{bmatrix} P_{00}^{-1}\bar{A}_{00}^T + \bar{A}_{00}P_{00}^{-1} - \mu_{00}B_0B_0^T & P_{00}^{-1} & P_{00}^{-1} \\ P_{00}^{-1} & -P_{10}^{-1}/\beta_{01}^0 & 0 \\ P_{00}^{-1} & 0 & -P_{01}^{-1}/\alpha_{01} \end{bmatrix} < 0. \tag{3.27}$$

If some transition rate is zero, the corresponding term involving zero rate in (3.25) is removed, and so are the corresponding row and column in (3.27). For example, if $\alpha_{01} = 0$, (3.27) becomes

$$\begin{bmatrix} P_{00}^{-1}\bar{A}_{00}^T + \bar{A}_{00}P_{00}^{-1} - \mu_{00}B_0B_0^T & P_{00}^{-1} \\ P_{00}^{-1} & -P_{10}^{-1}/\beta_{01}^0 \end{bmatrix} < 0.$$

Similarly, (3.18)-(3.20) can also be converted to LMI's that are affine in P_{00}^{-1}, P_{01}^{-1}, P_{10}^{-1}, P_{11}^{-1}, μ_{00}, μ_{01}, μ_{10}, and μ_{11}. ■

Remark 3.2 *The above results are for the basic case of FTCS's, and can be readily modified for the cases of multiple fault modes. For example, if $S_1 = S_2 = \{0, 1, 2\}$, to ensure stochastic stability, there are 9 inequalities in Theorem 3.1, and a typical one is*

$$\begin{bmatrix} P_{00}^{-1}\bar{A}_{00}^T P_{00} P_{00}^{-1}\bar{A}_{00}P_{00}^{-1} - \mu_{00}B_0B_0^T & P_{00}^{-1} & P_{00}^{-1} & P_{00}^{-1} & P_{00}^{-1} \\ P_{00}^{-1} & -P_{10}^{-1}/\beta_{01}^0 & 0 & 0 & 0 \\ P_{00}^{-1} & 0 & -P_{20}^{-1}/\beta_{02}^0 & 0 & 0 \\ P_{00}^{-1} & 0 & 0 & P_{01}^{-1}/\alpha_{01} & 0 \\ P_{00}^{-1} & 0 & 0 & 0 & P_{02}^{-1}/\alpha_{02} \end{bmatrix}$$

$< 0.$

Theorem 3.1 gives conditions on P_{ij}, $i, j \in \{0, 1\}$, to ensure that each single inequality in (3.17)-(3.20) has feasible solutions. The stabilizing controller $\mathbf{K} = \{K_0, K_1\}$ satisfying these 4 inequalities simultaneously can be generated by a randomization procedure presented in the next section.

3.5 Controller parameterization

Recall Lemma 3.3 and (3.11), and denote

$$\mathcal{K}^{\mathbf{P}} \triangleq \{\{K_0, K_1\} | K_0 \in \mathcal{W}_{00} \cap \mathcal{W}_{01},\ K_1 \in \mathcal{W}_{10} \cap \mathcal{W}_{11},\ \mathcal{W}_{ij} \triangleq \mathcal{G}_{P_{ij}B_j,Q_{ij}},\ i, j \in \{0, 1\}\}, \tag{3.28}$$

where $\mathbf{P} \triangleq \{P_{ij},\ i, j \in \{0, 1\}\}$. So $\mathcal{K}^{\mathbf{P}}$ is the set of stabilizing controllers associated with $\mathbf{P}$. Let $\mathcal{P} \triangleq \{\mathbf{P} | \mathbf{P}$ satisfies Theorem 3.1$\}$, the set of all $\mathbf{P}$ satisfying Theorem 3.1. $\mathbf{P} \in \mathcal{P}$ ensures that $\mathcal{W}_{ij} \neq \emptyset$, where $\emptyset$ denotes the empty set. The set of all stabilizing controllers is denoted as

$$\mathcal{K} \triangleq \{\text{All stabilizing } \mathbf{K}\} = \bigcup_{\mathbf{P} \in \mathcal{P}} \mathcal{K}^{\mathbf{P}}. \tag{3.29}$$

Figure 3.2 illustrates the relationship between $\mathcal{P}$ and $\mathcal{K}$: Each $\mathbf{K} \in \mathcal{K}$ corresponds to some $\mathbf{P} \in \mathcal{P}$; if $\mathcal{K}^{\mathbf{P}} \neq \emptyset$, all its elements correspond to and can be generated by $\mathbf{P}$ using a randomization procedure; if $\mathcal{K}^{\mathbf{P}} = \emptyset$, find another $\mathbf{P} \in \mathcal{P}$, and repeat the procedure.

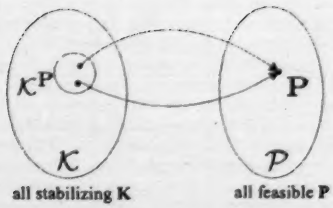

Figure 3.2: Relationship between $\mathcal{P}$ and $\mathcal{K}$.

The problem considered in this section is to check whether $\mathcal{K}^{\mathbf{P}} = \emptyset$ or not given $\mathbf{P} \in \mathcal{P}$; furthermore, if $\mathcal{K}^{\mathbf{P}} \neq \emptyset$, generate samples in $\mathcal{K}^{\mathbf{P}}$.

Based on (3.28), denote $\mathcal{K}_0^{\mathbf{P}} \triangleq \mathcal{W}_{00} \cap \mathcal{W}_{01}$ and $\mathcal{K}_1^{\mathbf{P}} \triangleq \mathcal{W}_{10} \cap \mathcal{W}_{11}$. Then $\mathcal{K}^{\mathbf{P}} = \mathcal{K}_0^{\mathbf{P}} \times \mathcal{K}_1^{\mathbf{P}}$, where '$\times$' denotes the Cartesian product. So $\mathcal{K}^{\mathbf{P}} \neq \emptyset$ if and only if $\mathcal{K}_0^{\mathbf{P}} \neq \emptyset$ and $\mathcal{K}_1^{\mathbf{P}} \neq \emptyset$. Take $\mathcal{K}_0^{\mathbf{P}}$ as an example for the following derivation, and the same procedure follows for $\mathcal{K}_1^{\mathbf{P}}$.

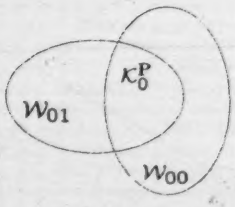

Figure 3.3: Illustration of controller generation.

As shown in Figure 3.3, the basic idea is to generate samples in $\mathcal{W}_{00} = \mathcal{G}_{P_{00}B_0,Q_{00}}$ and to test condition (3.14) for $\mathcal{W}_{01}$ to obtain $K_0 \in \mathcal{K}_0^{\mathbf{P}}$. Recall (3.11) and (3.28), and let the free parameters L and ρ be uniformly distributed random variables. $K_0 = g(L, \rho | P_{00}B_0, Q_{00}) \in \mathcal{W}_{00}$ can be generated by L and ρ, where $g(\cdot, \cdot | \cdot, \cdot)$ is defined in (3.5). Obviously, $\mathcal{K}_0^{\mathbf{P}} \neq \emptyset$ if and only if the following probability is nonzero:

$$\Pr\{K_0 \in \mathcal{K}_0^{\mathbf{P}} | K_0 \in \mathcal{W}_{00}\} = \Pr\{K_0 \text{ satisfies (3.14)} | K_0 \in \mathcal{W}_{00}\}. \tag{3.30}$$

Define an indicator function

$$I(L, \rho) = \begin{cases} 1, & K_0 \in \mathcal{K}_0^{\mathbf{P}} \text{ given } K_0 \triangleq g(L, \rho | P_{00}B_0, Q_{00}) \in \mathcal{W}_{00}; \\ 0, & \text{otherwise}, \end{cases}$$

and then $\Pr\{I(L, \rho) = 1\} = \Pr\{K_0 \in \mathcal{K}_0^{\mathbf{P}} | K_0 \in \mathcal{W}_{00}\}$. According to the Chernoff's bound [67, p. 123], when generating $N \geq \frac{\ln(2/\delta_2)}{2\epsilon_2^2}$ identically and independently distributed (i.i.d.) samples for $\delta_2 > 0$ and $\epsilon_2 > 0$, the following statistic provides an estimate of the

probability in (3.30):

$$\hat{P}_N = \frac{\sum_{i=1}^{N} I(L_i, \rho_i)}{N}, \tag{3.31}$$

where L_i and ρ_i denote i.i.d. samples of L and ρ respectively. Furthermore, it satisfies

$$\Pr\{|\Pr\{I(L,\rho)=1\} - \hat{P}_N| \leq \epsilon_2\} \geq 1 - \delta_2. \tag{3.32}$$

Suppose that ϵ_2 and δ_2 are so small that we can use the estimate $\hat{P}_N$ as the true probability in (3.30). So $\mathcal{K}_0^{\mathbf{P}} \neq \emptyset$ is equivalent to $\hat{P}_N > 0$, which solves the first problem of this section.

If $\mathcal{K}_0^{\mathbf{P}} \neq \emptyset$, we can then generate elements in $\mathcal{W}_{00}$ and test (3.14) to obtain samples in $\mathcal{K}_0^{\mathbf{P}}$. Recall Algorithm 3.1 in Section 3.2, and suppose M_1 stabilizing controllers are needed. The next problem is to determine the number of $K_0 \in \mathcal{W}_{00}$ to be tested in order to generate M_1 controllers $K_0 \in \mathcal{K}_0^{\mathbf{P}}$.

For M_2 i.i.d. samples L_i and ρ_i, denote $Y_i = I(L_i, \rho_i)$, $i = 1, \cdots, M_2$. So $\sum_{i=1}^{M_2} Y_i$ is the number of $K_0 \in \mathcal{K}_0^{\mathbf{P}}$ and subject to the following Binomial distribution:

$$\Pr\{\sum_{i=1}^{M_2} Y_i \geq M_1\} = \sum_{k=M_1}^{M_2} \binom{M_2}{k} (\hat{P}_N)^k (1-\hat{P}_N)^{M_2-k}. \tag{3.33}$$

Set a confidence level δ_3, and select M_2 to ensure $\Pr\{\sum_{i=1}^{M_2} Y_i \geq M_1\} \geq 1 - \delta_3$. This means that when testing M_2 samples in $\mathcal{W}_{00}$, M_1 samples of $K_0^i \in \mathcal{K}_0^{\mathbf{P}}$ are obtained with probability $1 - \delta_3$. The procedures of generating M_1 controllers are summarized in Algorithm 3.2.

Algorithm 3.2 - controller generation

1) Let $i = 0$.

2) For K_i, estimate $\Pr\{K_i \in \mathcal{K}_i^{\mathbf{P}} | K_i \in \mathcal{W}_{i0}\}$ by $\hat{P}_N$ in (3.31) for some small parameters ϵ_2 and δ_2. If $\hat{P}_N = 0$, no stabilizing controller exists and stop.

3) For a small confidence level δ_3, select M_2 such that

$$\sum_{k=M_1}^{M_2} \binom{M_2}{k} (\hat{P}_N)^k (1-\hat{P}_N)^{M_2-k} \geq 1 - \delta_3.$$

4) Generate M_2 samples in set $\mathcal{W}_{i0} = \mathcal{G}_{P_{i0}B_0,Q_{i0}}$. Test (3.14) if $i = 0$ or (3.15) if $i = 1$ for each sample, and record those stabilizing controllers in $\mathcal{K}_i^{\mathbf{P}}$.

5) Let $i = 1$, and follow steps 2) through 4) to generate the controller samples for K_1.

Remark 3.3 *Algorithm 3.2 still applies when there are multiple fault modes. For example, if $S_1 = S_2 = \{0, 1, 2\}$, there are 9 similar inequalities in Theorem 3.1; and each controller $\{K_0, K_1, K_2\}$ is in the intersection of three solution sets.*

Algorithm 3.2 generates the controllers for step 2 of Algorithm 3.1 in Section 3.2. The design procedure of FTCS's is finally established as follows by combining Algorithms 3.1 and 3.2.

Design procedure

1) Determine sample quantity $M_1 \geq \frac{1/\delta}{1/(1-\epsilon)}$ based on the precision parameters ϵ and δ.

2) Solve (3.21)-(3.24) in Theorem 3.1 for $\mathbf{P}$.

3) Use Algorithm 3.2 to generate M_1 stabilizing controllers corresponding to $\mathbf{P}$.

4) If M_1 controllers in $\mathcal{K}^{\mathbf{P}}$ are successfully generated, follow step 3) in Algorithm 3.1 on the generated controllers, and find the statistical optimum $\hat{\mathbf{K}}^*$. If $\mathcal{K}^{\mathbf{P}} = \emptyset$, go to step 2) to solve for an alternative $\mathbf{P}$.

If this procedure fails to find non-empty $\mathcal{K}^{\mathbf{P}}$, the system is said to be not stabilizable. However, this non-stabilizability can be checked before applying parameterization algorithms.

Remark 3.4 *Note that the freedom of $\mathbf{P}$ in (3.29) is not exploited in this design procedure though it is possible to obtain a set of feasible solutions $\mathbf{P}$ satisfying Theorem 3.1 by varying the settings in the LMI solver: the target value for the auxiliary convex program of the feasibility problem [71]. But this may lead to controllers with larger magnitudes which is not preferable in practice due to excessive control energy. So we do not solve a set of $\mathbf{P}$ and optimize among controllers with different orders of magnitudes.*

Remark 3.5 *This parameterization method can be extended to static output-feedback controllers $u(\eta(t), t) = K(\eta(t))y(t)$, provided that $D(\zeta(t)) = 0$ in (2.2). Using output-feedback controllers for this special case is equivalent to replacing $K(\eta(t))$ by $K(\eta(t))C(\zeta(t))$ in Lemma 3.1. Although Lemma 3.3 is not applicable due to different stability conditions in this case, an alternative parameterization result of matrix inequality can be applied and similar results can be derived [64, p. 29, Theorem 2.3.12]. However, for the general case of $D(\zeta(t)) \neq 0$, the stability conditions of the closed-loop system will contain matrix inverse terms involving $K(\eta(t))$. This is a major hurdle for extending the current results.*

3.6 Analysis of stabilizing controller set

In this section, the stabilizing controller set is analyzed based on its connections with the standard Linear Quadratic Regulator (LQR) problem. To see this relationship, FTCS model is converted to the form of JLS by representing the behaviors of two Markov processes into one, called the integrated Markov process $\phi(t)$ [70]; the solutions of LQR problem in this JLS form are then compared with the results in Section 3.4.

For the basic case of FTCS's, the augmented state space of $\phi(t)$ is $S_3 = S_2 \times S_1 = \{(0,0),\ (0,1),\ (1,0),\ (1,1)\}$, where the first element represents the FDI mode in S_2 and the second the fault mode in S_1. Let $\gamma_{(ij)(kl)}$ denote the transition rate of $\phi(t)$, which determines the transition probability of $\phi(t)$ from the augmented state (i,j) to (k,l) as shown in the following equation:

$$\phi(t) : p_{(ij)(kl)}(\triangle t) = \begin{cases} \gamma_{(ij)(kl)}\triangle t + o(\triangle t),\ i \neq j,\ k \neq l; \\ 1 - \gamma_{(ij)(kl)}\triangle t + o(\triangle t),\ i = j,\ k = l. \end{cases}$$

As shown in [70], $\gamma_{(ij)(kl)}$ can be derived from the transitions rates of $\zeta(t)$ and $\eta(t)$:

$$\gamma_{(ij)(kl)} = \begin{cases} \alpha_{jj} + \beta^j_{ii},\ i = k,\ j = l; \\ \beta^j_{ik},\ i \neq k,\ j = l; \\ \alpha_{jl},\ i = k,\ j \neq l; \\ 0,\ i \neq k,\ j \neq l. \end{cases} \tag{3.34}$$

For the basic case, the generator matrix F_ϕ of $\phi(t)$ is given by

$$H_\phi \triangleq [\gamma_{(ij)(kl)}]_{4\times 4} = \begin{bmatrix} -(\alpha_{00} + \beta^0_{00}) & \alpha_{01} & \beta^0_{01} & 0 \\ \alpha_{10} & -(\alpha_{11} + \beta^1_{00}) & 0 & \beta^1_{01} \\ \beta^0_{10} & 0 & -(\alpha_{00} + \beta^0_{11}) & \alpha_{01} \\ 0 & \alpha_{10} & \beta^1_{10} & -(\alpha_{11} + \beta^1_{11}) \end{bmatrix}.$$

By replacing $\zeta(t)$ and $\eta(t)$ with $\phi(t)$ in (3.1), the FTCS model becomes a standard JLS model:

$$\dot{x}(t) = A(\phi(t))x(t) + B(\phi(t))u(\phi(t),t), \tag{3.35}$$

The infinite-time LQR problem of JLS's aims to find a state-feedback controller to minimize the following objective:

$$\begin{aligned} J(t_0, x(t_0), u(t)) \ &= \ E\{\int_{t_0}^{\infty} [x^T(t)S(\phi(t))x(t) \\ &\quad + u^T(\phi(t),t)R(\phi(t))u(\phi(t),t)]dt | x(t_0), \phi(t_0)\}, \end{aligned} \tag{3.36}$$

where $S(\phi(t))$ and $R(\phi(t))$ denote state and control weighting matrices. For $\phi(t) = (i,j)$, denote $A_{ij} \triangleq A(\phi(t))$, $B_{ij} \triangleq B(\phi(t))$, $C_{ij} \triangleq C(\phi(t))$, $D_{ij} \triangleq D(\phi(t))$, $u_{ij}(t) \triangleq$

$u(\phi(t),t)$, $S_{ij} \triangleq S(\phi(t))$, and $R_{ij} \triangleq R(\phi(t))$. As system matrices depend on fault mode only, $A_{ij} = A_j$, $B_{ij} = B_j$, $C_{ij} = C_j$, and $D_{ij} = D_j$.

Using state-feedback controls in a switching structure, the LQR problem was solved by Theorem 5 in [53], which stated that the optimal state-feedback controller is

$$u_{ij}(t) = -R_{ij}^{-1} B_j^T P_{ij} x(t), (i,j) \in S_3, \tag{3.37}$$

where $P_{ij} > 0$ satisfies the coupled Algebraic Ricatti Equations (ARE's):

$$A_j^T P_{ij} + P_{ij} A_j - P_{ij} B_j R_{ij}^{-1} B_j^T P_{ij} + \gamma_{(ij)(ij)} P_{ij} + \sum_{(k,l)\neq(i,j)} \gamma_{(ij)(kl)} P_{kl} + S_{ij} = 0, \tag{3.38}$$

where $(i,j),(k,l) \in S_3$.

In JLS's, the number of switching controllers is equal to that of integrated Markov states of $\phi(t)$. For this JLS model in (3.35) converted from an FTCS model, there are 4 controllers designed corresponding to 4 states of $\phi(t)$ as given in (3.37). When $\phi(t) = (i,j)$, the following state-feedback gain is in use:

$$K_{ij} = -R_{ij}^{-1} B_j^T P_{ij}, \ (i,j) \in S_3. \tag{3.39}$$

In contrast, in FTCS's, the number of switching controllers is equal to that of fault modes so only 2 controllers exist for the basic case in (3.35). Therefore, JLS's have more design freedom while FTCS's are more restrictive, and the design methods of JLS's are not applicable to FTCS's. But the controller designed in FTCS's can be analyzed by the methods in JLS's considering that two controllers can be deemed as a special case of two pairs of identical controllers. For example, K_0 and K_1 in FTCS's are deemed to be K_0, K_0, K_1, and K_1 in JLS's.

Proposition 3.1 *(3.21)-(3.24) in Theorem 3.1 are equivalent to ARE's (3.38) of the LQR problem in JLS's. In other words,* $\mathbf{P} = \{P_{ij},\ i,j \in \{0,1\}\}$ *satisfies Theorem 3.1 if and only if it is a feasible solution of ARE's (3.38) corresponding to the following LQR weighting matrices:*

$$S_{ij} = \mu_{ij} P_{ij} B_j B_j^T P_{ij} - (\bar{A}_{ij}^T P_{ij} + P_{ij} \bar{A}_{ij} + \beta_{i(1-i)}^j P_{(1-i)j} + \alpha_{j(1-j)} P_{i(1-j)}), \tag{3.40}$$

$$R_{ij} = 1/\mu_{ij}, \ (i,j) \in S_3. \tag{3.41}$$

Proof: Substitute the system parameters into (3.38), we obtain 4 coupled ARE's. Note that the system matrices depend on the fault mode only, the second element of $\phi(t)$. For example, $A_{ij} = A_j$. Let us consider the following ARE for $\phi(t) = (0,0)$.

$$A_0^T P_{00} + P_{00} A_0 - P_{00} B_0 R_{00}^{-1} B_0^T P_{00} - (\alpha_{01} + \beta_{01}^0) P_{00} + \beta_{01}^0 P_{01} + \alpha_{01} P_{10} + S_{00} = 0.$$

Use $\bar{A}_{00} = A_0 - 0.5\beta_{01}^0 - 0.5\alpha_{01}$ defined in Theorem 3.1 to simplify this equation, and we have

$$\bar{A}_{00}^T P_{00} + P_{00} \bar{A}_{00} + \beta_{01}^0 P_{01} + \alpha_{01} P_{10} + S_{00} = P_{00} B_0 R_{00}^{-1} B_0^T P_{00}. \tag{3.42}$$

Let $R_{00} = 1/\mu_{00}$ and compare (3.42) with (3.26). If (3.42) holds, (3.26) obviously holds considering $S_{00} > 0$; if (3.26) holds, (3.42) also holds with

$$S_{00} = \mu_{00} P_{00} B_0 B_0^T P_{00} - (\bar{A}_{00}^T P_{00} + P_{00} \bar{A}_{00} + \beta_{01}^0 P_{10} + \alpha_{01} P_{01})$$

$$= P_{00} B_0 R_{00}^{-1} B_0^T P_{00} - (\bar{A}_{00}^T P_{00} + P_{00} \bar{A}_{00} + \beta_{01}^0 P_{10} + \alpha_{01} P_{01}) > 0.$$

So, (3.42) and (3.26) are equivalent. It immediately follows that (3.42) and (3.12) are equivalent. Similarly, we can establish the equivalence between (3.13)-(3.15) and the other three ARE's of (3.38) corresponding to $\phi(t) = (0,1), (1,0), (1,1)$. ■

Proposition 3.2 *The parameterization set $\mathcal{W}_{ij}$ in (3.28) contains an LQR controller of JLS's given in (3.37) corresponding to the weighting matrices in (3.40)-(3.41).*

Proof: Recall (3.28) and Lemma 3.3, if Theorem 3.1 holds, the feasible solutions for each inequality in (3.12)-(3.15) are parameterized by

$$\mathcal{W}_{ij} = \{K_{ij}' | K_{ij}' = -\rho_{ij}^{-1} B_j^T P_{ij} + \rho_{ij}^{-1/2} L_{ij} (\rho_{ij}^{-1} P_{ij} B_j B_j^T P_{ij} - Q_{ij})^{1/2},$$

$$\|L_{ij}\| < 1,\ \rho_{ij} \in (0,\ \rho_{ij\max})\},\ i \in S_2,\ j \in S_1, \tag{3.43}$$

where L_{ij} and ρ_{ij} are free parameters and $\rho_{ij\max}$ is calculated by (3.6) in Lemma 3.3. Furthermore, by Lemma 3.3, $\rho_{ij} \in (0,\ \rho_{ij\max})$ if and only if it satisfies (3.7): $\rho_{ij}^{-1} P_{ij} B_j B_j^T P_{ij} - Q_{ij} > 0$.

ρ_{ij} may take the value of μ_{ij}^{-1} because

$$\mu_{ij} P_{ij} B_j B_j^T P_{ij} > Q_{ij},\ i \in S_2,\ j \in S_1. \tag{3.44}$$

To see this inequality (3.44), take $i = 0$ and $j = 0$ as an example, and substitute the definition of Q_{00} in (3.16). (3.44) then becomes (3.26), which has been proved in Theorem 3.1.

Let the free parameter $L_{ij} = 0$ and the corresponding element in $\mathcal{W}_{ij}$ is

$$K'_{ij} = -\mu_{ij} B_j^T P_{ij},\ i \in S_2,\ j \in S_1. \tag{3.45}$$

Considering (3.41) in Proposition 3.1,

$$K'_{ij} = -R_{ij}^{-1} B_j^T P_{ij},\ i \in S_2,\ j \in S_1 \tag{3.46}$$

which is obviously the LQR controller in (3.39). ■

These two propositions are derived from Theorem 3.1 and Lemma 3.3, and the proofs are given in the appendix. Proposition 3.2 shows that $\mathcal{W}_{00}$ and $\mathcal{W}_{01}$ contain an LQR controller of JLS's, and these sets are around an LQR controller; so the parameterization set $\mathcal{K}_0^{\mathrm{P}}$ is also around an LQR controller. This connection provides a meaningful interpretation of the stabilizing controller set found in Section 3.5.

3.7 Synthesis of generator matrices

Clearly, the generator matrices of $\zeta(t)$ and $\eta(t)$ are crucial parameters in the model of FTCS's. In this section, synthesis methods are presented based on two structures of Markov processes and the knowledge of failure rates and FDI history data.

Let $Y(t)$ denote a homogenous continuous-time Markov process in a finite state space S_Y. Let $T_0, T_1, T_2, \cdots$ denote transition times and $Y_0, Y_1, Y_2, \cdots$ the successive states visited by $Y(t)$. If $Y_n = i$, $[T_n, T_{n+1})$ is called sojourn interval, and $T_{n+1} - T_n$ the sojourn time at state i, $i \in S_Y$, $n \in \mathbb{N}$. Markov process theory states that $\{Y_n, n \in \mathbb{N}\}$ forms a Markov chain, and $T_{n+1} - T_n$ follows exponential distribution with parameter depending on Y_n only [25, Chap. 8]. This is the first structure of a Markov process.

Let Q_Y denote the generator matrix of $Y(t)$ and $Q_Y(i,j)$ its transition rate. The transition probabilities of Y_n are

$$\Pr\{Y_{n+1} = j | Y_n = i\} = \frac{Q_Y(i,j)}{Q_Y(i,i)},\ i \neq j, \tag{3.47}$$

and $\Pr\{Y_{n+1} = i | Y_n = i\} = 0$, $i, j \in S_Y$. If $Q_Y(i,i) = 0$, state i is absorbing, and $\Pr\{Y_{n+1} = j | Y_n = i\} = 0$ for all $j \in S_Y$. The sojourn time distribution at state i is

$$\Pr\{T_{n+1} - T_n > t | Y_n = i\} = e^{-Q_Y(i,i)t}. \tag{3.48}$$

Note that $Q_Y(i,j) \geq 0$, and $Q_Y(i,i) = \sum_{j \in S_Y} Q_Y(i,j), i \neq j$.

The second structure uses competitions among independent exponential random variables to determine sojourn times and successive transition states. When $Y(t) = i$, an exponentially-distributed random variable τ_{ij} with rate $Q_Y(i,j)$ is associated with transition to j in S_Y. The transition can be viewed as a competition process among τ_{ij}, $j \in S_Y$: the state associated with the minimum of τ_{ij} is the successive state visited by $Y(t)$, and this minimum value gives the sojourn time at i. Based on the property of independent exponential random variables [72, p. 243], (3.47) and (3.48) can be derived under this structure.

Using the Markov process $\zeta(t)$ to describe fault occurrences requires the assumption of constant failure rates, or equivalently, exponential distribution of lifetime, which is generally valid for the majority of component lifetime [21]. The generator matrix of $\zeta(t)$ can be synthesized based on the second structure and failure rates. In the state space S_1 of $\zeta(t)$, 0 usually represents fault-free mode, and other states describe specific faults and may also describe their combinations. The transitions of $\zeta(t)$ may represent fault occurrences, repairs, or recoveries from intermediate faults depending on transition modes and directions.

For example, for a system with two types of faults, S_1 can be defined as $\{0,1,2,3\}$, where each mode represents respectively fault-free mode, fault type I, fault type II, and their simultaneous occurrences. The transitions from mode 0 to 1 or 2 represent the occurrences of fault type I or II respectively, while the transitions of opposite directions represent repairs or recoveries from these faults. In cases of multiple faults that may occur at a particular mode, there exist competitions among exponential lifetime random variables: the fault occurring first with minimum lifetime makes $\zeta(t)$ jump to the corresponding mode in S_1, and the minimum lifetime gives its sojourn time. So, the transition rates in the upper-triangular part of F correspond to failure rates; and those in the lower-triangular part represent the rates of repairs or recoveries. Let the failure rates of two faults be denoted by λ_1 and λ_2 respectively, and the generator matrix of $\zeta(t)$ is

$$H_\zeta = \begin{bmatrix} -(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 & 0 \\ 0 & -\lambda_2 & 0 & \lambda_2 \\ 0 & 0 & -\lambda_1 & \lambda_1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

where the transition rates in lower-triangular part are all zeros as no repair or intermediate fault is assumed.

$\eta(t)$ models FDI results, and its state space S_2 is usually identical to S_1. Its generator matrix can be estimated using FDI history data based on the first structure of Markov processes. This history data should record the transition states and sojourn times of FDI under

known fault modes, which can be obtained by experimental testing of FDI schemes. Owing to (3.47)-(3.48), it suffices to estimate the transition probabilities and the means of sojourn time distributions in order to determine the generator matrix of $\eta(t)$.

When $\zeta(t) = k$ and $\eta(t) = i$, the sample sojourn time of $\eta(t)$ at i is recorded as $\tau_i^{(l)}$, $l = 1, 2, \cdots, N$. The sample average

$$\bar{\tau}_i = \sum_{l=1}^{N} \tau_i^{(l)} / N$$

converges to $1/\beta_{ii}^k$ in probability 1 as $N \to \infty$ based on the law of large numbers and (3.48). Let $\hat{\beta}_{ii}^k = 1/\bar{\tau}_i$ denote the estimate of β_{ii}^k. If there is no transition from state i for $\eta(t)$, this state is deemed to be absorbing, and $\hat{\beta}_{ii}^k = 0$ in this case.

The transition probability can be estimated by transition frequencies. If there are M transitions of $\eta(t)$ to mode j within N transitions leaving i in FDI history data, the transition frequency M/N converges to transition probability with probability 1 as $N \to \infty$. Using (3.47), the transition rate from i to j is estimated as

$$\hat{\beta}_{ij}^k = \hat{\beta}_{ii}^k M/N.$$

Using this method, all elements in the generator matrix of $\eta(t)$ can be estimated. Moreover, as in (3.32), to ensure specific estimate precisions, the lower bound of sample quantity N can be determined using the Chernoff's bound.

Remark 3.6 *Fault effects on system dynamics are described by different system matrices in the dynamic model (3.1), $A(\zeta(t))$, $B(\zeta(t))$, $C(\zeta(t))$, and $D(\zeta(t))$ depending on $\zeta(t)$. The FDI scheme can be designed by standard model-based methods using these dynamic models [73]. Although some iterative algorithms exist to obtain a sequence estimate of Markov states based on the probabilistic description of system modes, the computational cost is not suitable for online implementation and controller reconfiguration, and the algorithms are designed for a discrete-time Markov chain only [74]. The transition characteristics of FDI mode can be described by a Markov process from the perspective of closed-loop stability of the reconfigured system [6]. But it is necessary to have FDI history data available for estimating Markov transition rates.*

3.8 An illustrative example

Consider a longitudinal vertical takeoff and landing aircraft model in the form of (2.2) with the following system matrices [13]. The subscript '0' represents the fault-free mode and '1'

the faulty mode. In the faulty mode, the actuator failure is considered, and the effectiveness of the first actuator is reduced by half as reflected in B_1.

$$A_0 = \begin{bmatrix} -0.0366 & 0.0271 & 0.0188 & -0.4555 \\ 0.0482 & -1.01 & 0.0024 & -4.0208 \\ 0.1002 & 0.3681 & -0.707 & 1.420 \\ 0 & 0 & 1.0 & 0 \end{bmatrix}, \quad A_1 = A_0,$$

$$B_0 = \begin{bmatrix} 0.4422 & 0.1761 \\ 3.5446 & -7.5922 \\ -5.52 & 4.49 \\ 0 & 0 \end{bmatrix}, B_1 = \begin{bmatrix} 0.2211 & 0.1761 \\ 1.7723 & -7.5922 \\ -2.76 & 4.49 \\ 0 & 0 \end{bmatrix}, C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, C_1 = C_0.$$

The generator matrices of $\zeta(t)$ and $\eta(t)$ are:

$$H_\zeta = \begin{bmatrix} -0.0017 & 0.0017 \\ 0 & 0 \end{bmatrix}, H_\eta^0 = \begin{bmatrix} -0.0204 & 0.0204 \\ 3.9039 & -3.9039 \end{bmatrix}, H_\eta^1 = \begin{bmatrix} -2.9925 & 2.9925 \\ 0.0515 & -0.0515 \end{bmatrix}.$$

According to H_ζ, the mean lifetime before fault occurrence is 1/0.0017=588.24 minutes, and the fault mode is absorbing as shown in the second zero row of H_ζ, i.e., there is no repair or recovery from intermediate fault. For FDI, according to the first row of H_η^0, when the system is in fault-free mode, the mean time of a false alarm is 1/0.0204=49.02 minutes; and according to its second row, the mean time of returning to correct detection after a false alarm is 1/3.9039=0.2562 of a minute. H_η^1 can be interpreted similarly: the mean time of a missing detection is 1/0.0515 = 19.42 minutes, and the mean time of returning to correct detection after a missing detection is 1/2.9925 =0.3342 of a minute.

The conditions in Theorem 3.1 for P_{ij} are solved as follows:

$$P_{00} = \begin{bmatrix} 0.0114 & 0.0009 & -0.0028 & -0.0065 \\ 0.0009 & 0.0043 & -0.0011 & 0.0004 \\ -0.0028 & -0.0011 & 0.0099 & 0.0079 \\ -0.0065 & 0.0004 & 0.0079 & 0.0208 \end{bmatrix},$$

$$P_{01} = \begin{bmatrix} 3.5840 & 0.1916 & -0.5806 & -1.1955 \\ 0.1916 & 3.2196 & -0.2804 & -0.0447 \\ -0.5806 & -0.2804 & 3.4266 & 1.1760 \\ -1.1955 & -0.0447 & 1.1760 & 4.9369 \end{bmatrix},$$

$$P_{10} = \begin{bmatrix} 0.0484 & 0.0050 & -0.0073 & -0.0084 \\ 0.0050 & 0.0619 & -0.0147 & 0.0052 \\ -0.0073 & -0.0147 & 0.0703 & 0.0102 \\ -0.0084 & 0.0052 & 0.0102 & 0.0669 \end{bmatrix},$$

$$P_{11} = \begin{bmatrix} 2.7515 & -0.1065 & -1.0816 & -1.2975 \\ -0.1065 & 3.5939 & -0.1549 & -0.0833 \\ -1.0816 & -0.1549 & 3.4801 & 1.6071 \\ -1.2975 & -0.0833 & 1.6071 & 3.8389 \end{bmatrix}.$$

Based on Proposition 1, these P_{ij} correspond the following LQR weighting matrices S_{ij} and R_{ij}:

$$S_{00} = \begin{bmatrix} 0.0120 & 0.0184 & -0.0303 & -0.0113 \\ 0.0184 & 0.0351 & -0.0533 & -0.0144 \\ -0.0303 & -0.0533 & 0.0884 & 0.0279 \\ -0.0113 & -0.0144 & 0.0279 & 0.0165 \end{bmatrix},$$

$$S_{01} = \begin{bmatrix} 213.7 & 1161 & -954.4 & -307.4 \\ 1161.0 & 7689.3 & -5618.3 & -1764.3 \\ -954.4 & -5618.3 & 4436.9 & 1416.5 \\ -307.4 & -1764.3 & 1416.5 & 460.1 \end{bmatrix},$$

$$S_{10} = \begin{bmatrix} 0.2133 & 0.3874 & -0.4153 & 0.0212 \\ 0.3874 & 2.7692 & -2.4173 & 0.1968 \\ -0.4153 & -2.4173 & 2.7225 & -0.0830 \\ 0.0212 & 0.1968 & -0.0830 & 0.1956 \end{bmatrix},$$

$$S_{11} = \begin{bmatrix} 267.1 & 1348.6 & -1027.9 & -478 \\ 1348.6 & 9117.3 & -5859.5 & -2690.3 \\ -1027.9 & -5859.5 & 4154.7 & 1921.8 \\ -478 & -2690.3 & 1921.8 & 891.3 \end{bmatrix},$$

$$R_{00} = 0.0676,\ R_{01} = 0.0913,\ R_{10} = 0.1570,\ R_{11} = 0.0911.$$

Following the design procedure with $\epsilon = 0.02$ and $\delta = 0.02$, 194 sample controllers are generated and evaluated with respect to MTTF. It is found that the following approximately optimal controller $\hat{\mathbf{K}}^* = \{\hat{K}_0^*,\ \hat{K}_1^*\}$ achieves MTTF = 197.3208 minutes with $\Pr\{\Pr\{\psi(\mathbf{K}^*) > \psi(\hat{\mathbf{K}}^*)\} \leq 0.02\} \geq 0.98$, where $\psi(\mathbf{K}^*)$ denotes the optimal MTTF with the optimal controller $\mathbf{K}^*$:

$$\hat{K}_0^* = \begin{bmatrix} -0.6566 & -0.7359 & 2.0731 & 1.1449 \\ 0.4176 & 1.3777 & -1.1316 & -1.0322 \end{bmatrix},$$

$$\hat{K}_1^* = \begin{bmatrix} -0.1117 & 0.2114 & 0.1399 & 0.4621 \\ 0.0621 & 0.5747 & -0.1667 & -0.3248 \end{bmatrix}.$$

For comparison, arbitrarily select another stabilizing controller $\mathbf{K} = \{K_0,\ K_1\}$ with MTTF = 55.8319 minutes:

$$K_0 = \begin{bmatrix} -3.2572 & -1.8991 & 8.0921 & 6.7639 \\ -0.8941 & 0.8646 & 1.0997 & 1.1335 \end{bmatrix},$$

$$K_1 = \begin{bmatrix} 0.0272 & 0.2312 & 0.0945 & 0.0146 \\ 0.0427 & -0.0603 & -0.0534 & -0.5202 \end{bmatrix}.$$

To compare the time-domain performance of these two controllers, a white noise disturbance is applied to the system. With initial state $x(0) = [2 \quad -2 \quad 2 \quad -2]^T$, output trajectories are shown in Figures 3.4 and 3.5, where $\zeta(t)$ remains at fault-free mode 0, and

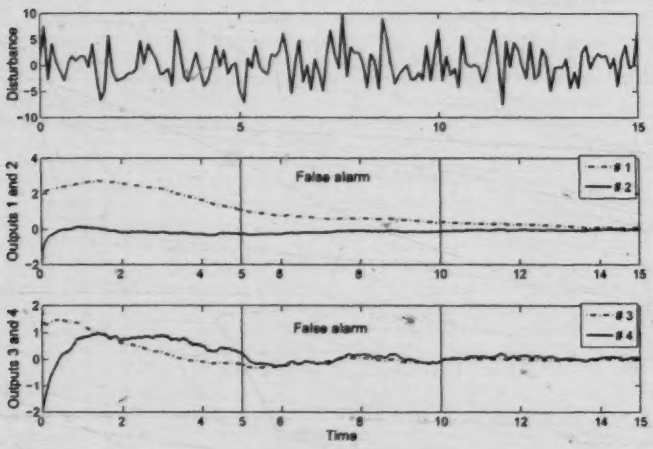

Figure 3.4: Output trajectories when using $\hat{\mathbf{K}}^*$.

$\eta(t)$ is manually set to 1 such that FDI gives false alarms when $5 \leq t < 10$. In fact, the sample paths of $\zeta(t)$ and $\eta(t)$ can be generated based on their generator matrices. But, the possibility of observing fault occurrences or false alarms in a short time is very small. In order to study system responses under false alarms, we manually set the transitions of $\eta(t)$. Moreover, to examine the robust performance of controllers, system matrices are perturbed probabilistically around their nominal values during the simulation.

As shown in Figures 3.4 and 3.5, output trajectories are converging and disturbances attenuated by both controllers; overall, $\hat{\mathbf{K}}^*$ seems to have better disturbance attenuation effects. This can be further validated by comparing the closed-loop $\mathcal{H}_\infty$ norms. For $\hat{\mathbf{K}}^*$, the nominal closed-loop $\mathcal{H}_\infty$ norm is 0.1294 when $\eta(t) = 0$ and 0.1565 when $\eta(t) = 1$; for $\mathbf{K}$, it is 0.1088 when $\eta(t) = 0$ and 0.2178 when $\eta(t) = 1$. If probabilistic modeling uncertainties are considered, for $\hat{\mathbf{K}}^*$, the probabilities that the $\mathcal{H}_\infty$ norm is no greater than 1 are 0.6467 and 0.7600 when $\eta(t) = 0$ and 1 respectively [46]; for $\mathbf{K}$, the probabilities are 0.6328 and 0.1043 respectively, much worse than $\hat{\mathbf{K}}^*$ especially under false alarms. This finding is not surprising because in this example the $\mathcal{H}_\infty$ norm under probabilistic uncertainties has been used as a control objective in the definition of a reliability function. The case for missing detection of FDI under fault occurrence can be studied in a similar way, which is not included for brevity.

The reliability functions of FTCS's for these two controllers are shown in Figure 3.6, and the reliability shows great improvement by using $\hat{\mathbf{K}}^*$. To verify $\Pr\{\Pr\{\psi(\mathbf{K}^*) >$

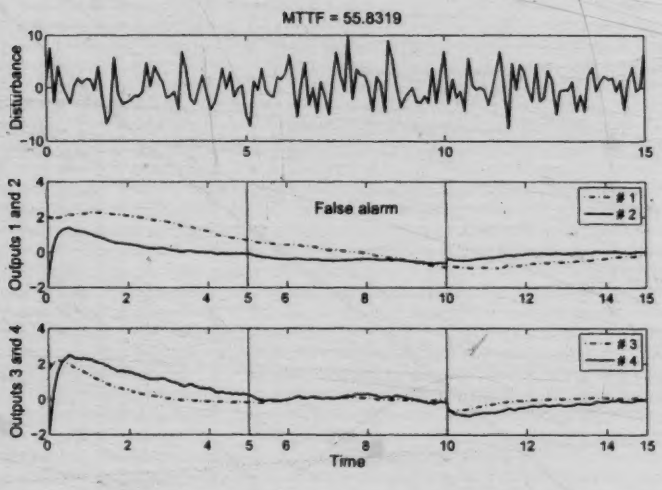

Figure 3.5: Output trajectories when using $\mathbf{K}$.

$\psi(\hat{\mathbf{K}}^*)\} \leq 0.02\} \geq 0.98$, 1000 stabilizing controller samples are generated, and the MTTF of the FTCS for each controller is calculated as shown in Figure 3.7. From this figure, it is found that only one controller has better MTTF than $\hat{\mathbf{K}}^*$. Therefore, the randomized algorithm gives a valid estimate of optimum with the specified precision.

3.9 Conclusion

This chapter presents a probabilistic design method of FTCS's based on the stability and reliability criteria. The basic idea is to develop a stabilizing controller parameterization set and to apply the randomized algorithms to find the statistically optimal controller in terms of system reliability. The stabilization conditions are given in the form of LMI's, and the free parameters in the controller parameterization set are real matrices and scalars, which is convenient for numerical implementation. An example is presented, and the results show that a statistically optimal controller with highest reliability can be obtained by this method.

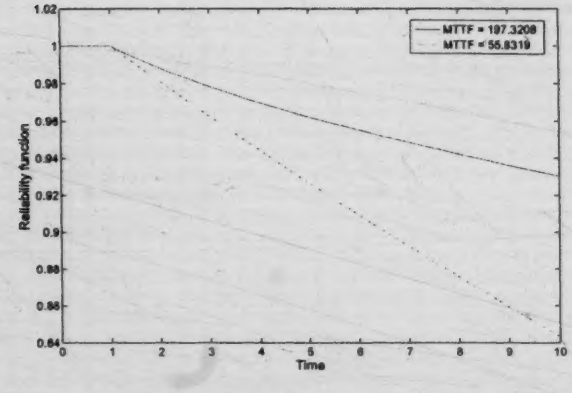

Figure 3.6: Compare reliability functions when using $\hat{\mathbf{K}}^*$ and $\mathbf{K}$.

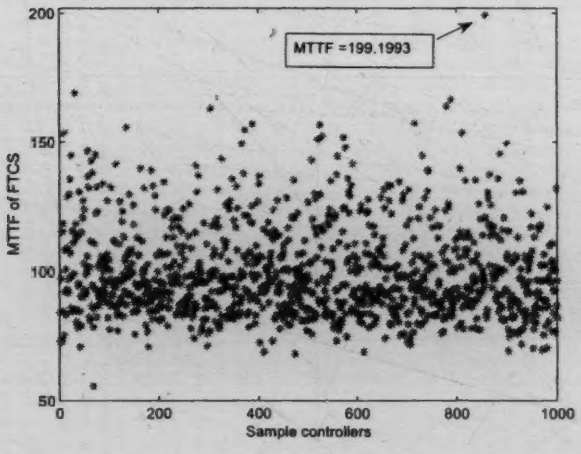

Figure 3.7: MTTF of FTCS for 1000 generated stabilizing controllers.

Chapter 4

Two-stage controller design for MTTF*

4.1 Introduction

The reliability-based design is basically an optimization problem with respect to reliability index. For example, in the active control of civil engineering structures, reliability-based design is usually converted to covariance control or classical optimization problems using approximate reliability measures [75, 44]. Similarly, reliable control aims to guarantee stability and/or control performance under component faults [19]. However, a valid reliability index of FTCS's is often evaluated from stochastic models and cannot be readily converted to a control objective. A reliability-based reconfiguration strategy was recently developed for FTCS's by optimizing system structure to improve reliability but the effects of control actions were not considered [76].

Owing to the numerical procedures of building and solving stochastic reliability models, it is generally difficult to write the reliability index as an analytical function of controller parameters. In order to overcome this difficulty, stabilizing controller parameterization and randomization-based methods were developed in Chapter 3 to find the statistically optimal controller with respect to reliability. Its advantage is the stabilizing property of designed controllers; but the algorithm may need to generate a large set of controllers for optimization purpose, which may lead to high computation burden.

This chapter discusses a new controller design method to optimize a long-run reliability index, MTTF. This index is evaluated based on probabilistic control performance characteristics, which are used to relate controller to MTTF. The basic idea is to perform MTTF optimization in two stages: 1) a gradient-based search is performed on control performance

*Results presented in this chapter has been submitted to the *International Journal of Robust and Nonlinear Control*, revised and under review.

characteristics which are updated along the fastest increasing direction of MTTF; 2) the updated control performance characteristics are then transmitted to a controller design algorithm, which updates controller accordingly to satisfy these control performance characteristics. Each design stage is completed by one iterative algorithm, and two algorithms are carried out alternately to complete controller design. This two-stage design overcomes the difficulty caused by the nonexistence of analytical objective functions of MTTF with respect to controller parameters. It also has relatively fast convergence because of the gradient information used in the algorithm.

The control performance is characterized by a probabilistic $\mathcal{H}_\infty$ criterion, defined as the probability that the $\mathcal{H}_\infty$ norm is within specified threshold when assuming bounded random uncertainties. $\mathcal{H}_\infty$ norm is suitable for describing long-term static control performance; when transient behaviors are of interest, a model-matching structure can be adopted to represent transient performance using $\mathcal{H}_\infty$ norm. To design a controller for this probabilistic $\mathcal{H}_\infty$ criterion, a sequential randomized algorithm is adopted. This algorithm iteratively updates controller based on uncertainty samples, and is effective to handle probabilistic robust performance. For example, it has been used for robust guaranteed cost control [48], robust linear matrix inequities problem [77], linear parameter varying design [78], and searching for common Lyapunov functions [79]. In this chapter, probabilistic $\mathcal{H}_\infty$ control is considered, and the main difference from previous work lies in the introduction of a weighted composite violation function to handle multiple regime models in FTCS's; both state feedback and two-degree-of-freedom (2DOF) controls are discussed; and both the convexity of violation function and the convergence of algorithms are proved for this new problem.

The remainder of this chapter is organized as follows: System model is introduced in Section 4.2; controller design algorithms are discussed in Sections 4.3 and 4.4 for state feedback control and 2DOF control respectively; Section 4.5 addresses output feedback controller design when state information is unavailable; and an example is finally given in Section 4.6 to demonstrate the method.

4.2 Problem formulation

4.2.1 System model

The general Markov model of FTCS's is given by 2.2 in Chapter 2. As state-feedback controller is considered in this chapter, it can be reduced to the following equations by

removing the output equation:

$$\begin{cases} \dot{x}(t) = A(\zeta(t), \Delta)x(t) + B(\zeta(t), \Delta)u(\eta(t), t) + E(\zeta(t), \Delta)w(t), \\ z(t) = C(\zeta(t), \Delta)x(t) + D(\zeta(t), \Delta)u(\eta(t), t) + F(\zeta(t), \Delta)w(t), \end{cases} \tag{4.1}$$

where $x(t) \in \mathbb{R}^n, z(t) \in \mathbb{R}^m, u(\eta(t), t) \in \mathbb{R}^p$, and $w(t) \in \mathbb{R}^q$ denote system state, regulated output representing control performance, control input, and exogenous input respectively. $\mathbb{R}^n$ denotes the real vector space with dimension n. A, B, C, D, E, and F denote system matrices with compatible dimensions determined by discrete modes $\zeta(t)$ and $\eta(t)$, and affected by uncertainty parameter Δ. $\zeta(t)$ and $\eta(t)$ are assumed to be two continuous-time Markov processes. $\Delta \in \mathbb{R}^l$ is assumed to be a random vector with known probability distribution in a bounded set Ω, and the entries in system matrices are affected by the elements in Δ.

Remark 4.1 *Different from a measured output, $z(t)$ is the regulated output to characterize control performance. For example, in tracking control, $z(t)$ can be taken as the tracking error between controlled output and reference command input. $w(t)$ contains exogenous inputs to the system, such as reference command input and disturbances, whose effects on $z(t)$ are undesirable and to be suppressed by designing controllers. As $w(t)$ may contain various types of signals, it cannot be described by a Gaussian white noise, and therefore Ito stochastic differential equations are not applicable here.*

Remark 4.2 *The required assumption to describe FDI mode $\eta(t)$ as a Markov process is the memoryless Markov property [25, p. 233]. According to [15, section 2.1], if FDI schemes are designed based on single sample hypothesis tests and the noise statistics are white, this assumption is valid. For general FDI schemes, it is difficult to check this memoryless assumption based on their designs, and semi-Markov processes can be used instead as discussed in Chapter 5. If FDI history data is available for estimating empirical sojourn time distribution, the assumption can be tested by checking whether sojourn time follows exponential distribution or not. Under the assumption that FDI modes can be modeled by a semi-Markov process, the exponential distribution implies that a Markov process is a valid model [25, p. 316]; considering that semi-Markov assumption is usually acceptable for describing FDI modes, this sojourn time distribution test can also be used in general to check Markov assumption.*

Remark 4.3 *Model (4.1) is a linear dynamical system subject to Markov switchings and has been discussed in many references. According to [7, p. 32], [80, p. 117], and [81,*

p. 143], the existence conditions of a unique solution are the Lipschitz and linear growth conditions of the right hand side of (4.1) with respect to x. For a general setting, a rigorous proof is provided in [82, p. 81] for stochastic differential equations with Markov switchings, and model (4.1) can be deemed as one of its special cases.

A static state feedback controller in a switching structure is considered for FTCS's. Here, static means that the controller is a pure gain. If the exogenous input $w(t)$ contains unknown disturbances only, the controller is composed of a set of state feedback gains, denoted by $\mathbf{K} \triangleq \{K_j,\ j \in S_2\}$, and $u(\eta(t), t) = K_j x(t)$ when $\eta(t) = j$. With this controller, the closed-loop system equations become

$$\begin{cases} \dot{x}(t) = [A(\zeta(t), \Delta) + B(\zeta(t), \Delta)K_{\eta(t)}]x(t) + E(\zeta(t), \Delta)w(t), \\ z(t) = [C(\zeta(t), \Delta) + D(\zeta(t), \Delta)K_{\eta(t)}]x(t) + F(\zeta(t), \Delta)w(t). \end{cases} \tag{4.2}$$

where $K_{\eta(t)}$ represents K_j when $\eta(t) = j$.

On the other hand, if the exogenous input contains known reference command input, the controller may be in a 2DOF structure, denoted by $\mathcal{K} \triangleq \{(K_j, L_j),\ j \in S_2\}$, and $u(\eta(t), t) = K_j x(t) + L_j w(t)$ when $\eta(t) = j$. The term 2DOF means there are two control gains involved for state feedback and reference feedforward respectively. The closed-loop system equations become

$$\begin{cases} \dot{x}(t) = [A(\zeta(t), \Delta) + B(\zeta(t), \Delta)K_{\eta(t)}]x(t) + [E(\zeta(t), \Delta) + B(\zeta(t), \Delta)L_{\eta(t)}]w(t), \\ z(t) = [C(\zeta(t), \Delta) + D(\zeta(t), \Delta)K_{\eta(t)}]x(t) + [F(\zeta(t), \Delta) + D(\zeta(t), \Delta)L_{\eta(t)}]w(t). \end{cases} \tag{4.3}$$

The closed-loop system (4.2) or (4.3) contains two discrete modes $\zeta(t)$ and $\eta(t)$, also referred to as system regime modes. For fixed regime modes $\zeta(t) = i$ and $\eta(t) = j$, (4.2) or (4.3) is reduced to a linear uncertain system, and the transfer function from $w(t)$ to $z(t)$ is denoted by $G_{ij}(s, \Delta)$, called a regime model. So, (4.2) or (4.3) represents a collection of linear uncertain regime models denoted by $\{G_{ij}(s, \Delta), i \in S_1, j \in S_2\}$. Owing to possible incorrect FDI decisions, each controller K_j or (K_j, L_j) may be used for $N_1 + 1$ possible regime models: $G_{0j}(s, \Delta), \cdots, G_{N_1 j}(s, \Delta)$, $j \in S_2$. This is the major difference from jump linear systems, where the number of controllers equals that of regime models [54].

4.2.2 Control performance characterization

The control performance of $G_{ij}(s, \Delta)$ is assumed to be represented by a model-based criterion, such as system norms. Let $\varpi(G_{ij}(s, \Delta))$ denote the performance measure calculated for fixed regime modes $\zeta(t) = i$, $\eta(t) = j$, and a particular uncertainty sample Δ. The

allowable performance bound when $\zeta(t) = i$ is denoted by ρ_i. To take into account the random uncertainty Δ, a probabilistic performance description is considered for each regime model:

$$\gamma_{ij} \triangleq \Pr\{\varpi(G_{ij}(s, \Delta)) \leq \rho_i\},\ i \in S_1,\ j \in S_2. \tag{4.4}$$

For fixed $\zeta(t) = i$ and $\eta(t) = j$, probabilistic performance γ_{ij} can be estimated by

$$\gamma_{ij} \approx \frac{1}{N} \sum_{h=1}^{N} 1_{\varpi(G_{ij}(s,\Delta_h))\leq\rho_i}, \tag{4.5}$$

where Δ_h denotes the generated uncertainty sample according to its distribution, and G_{ij} (s, Δ_h) the close-loop transfer function. The indicator function $1_{\varpi(G_{ij}(s,\Delta_h))\leq\rho_i}$ equals 1 if $\varpi(G_{ij}(s, \Delta_h)) \leq \rho_i$ and 0 otherwise. N can be determined based on the allowable estimation error using statistical theory, such as Chernoff's bound [46]. If $N \geq \frac{\ln(2/\delta)}{2\epsilon^2}$, the following inequality holds:

$$\Pr\{|\gamma_{ij} - \frac{1}{N} \sum_{h=1}^{N} 1_{\varpi(G_{ij}(s,\Delta_h))\leq\rho_i}| \leq \epsilon\} \geq 1 - \delta.$$

If N is large enough, the estimation errors ϵ and δ can be ignored, and (4.5) can be deemed as the true probabilistic performance γ_{ij}.

Model-based criteria are mainly defined for steady-state or long-term performance. When regime modes are under fast transitions, transient performance is of interest and should also be reflected in control performance characterization. In this chapter, $\mathcal{H}_\infty$ norm is selected as the model-based criterion and can represent transient performance by using suitable weighting functions [83]. But, adjusting weighting functions may need trial and error, and an alternative method is adopted here based on model-matching $\mathcal{H}_\infty$ design [47]. Its basic idea is shown in Figure 4.1: the required transient performance is represented by a desired model, and the controller is designed to minimize the $\mathcal{H}_\infty$ norm from reference input to mismatch error signal. The reference input can be chosen as the exogenous input $w(t)$, and mismatch error as $z(t)$. In this way, $\mathcal{H}_\infty$ controller can be designed for transient performance. The controller may take the 2DOF state feedback structure, and the closed-loop equations have similar forms as (4.3).

4.2.3 MTTF gradient

Reliability criteria presented in Chapter 2 provide quantitative measures on overall long-term performance of FTCS's. To avoid high costs of emergency repairs between periodic

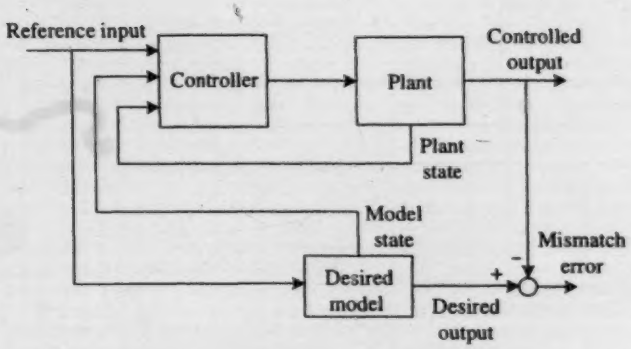

Figure 4.1: Model-matching diagram.

maintenance activities, the probability of failure within a maintenance period should be reduced to a certain level. For this purpose, the interested problem is to design a controller that achieves suboptimal MTTF exceeding $\overline{\text{MTTF}}$, where $\overline{\text{MTTF}}$ represents minimum MTTF requirement and can be determined based on maintenance period.

For the sake of reliability evaluation, a semi-Markov process $X^{\text{R}}(t)$ was constructed in Chapter 2. Its state space S_{R} is composed of operational or up states and a unique down state. The transition characteristics of $X^{\text{R}}(t)$ is defined by its semi-Markov kernel $Q(X_k, X_h, t)$ based on probabilistic performance γ_{ij}, where X_k and X_h represent the states of $X^{\text{R}}(t)$. The detailed definition and derivation of $Q(X_k, X_h, t)$ can be found in Chapter 2. Based on $X^{\text{R}}(t)$, MTTF can be calculated by [27]:

$$\text{MTTF} = p_0^T (I - P_{\text{up}})^{-1} \mu, \tag{4.6}$$

where I denotes the identity matrix with compatible dimensions, p_0 the vector of initial probability distribution of $X^{\text{R}}(t)$, P_{up} its limiting transition probability matrix, and μ the vector of expected sojourn time at up states of $X^{\text{R}}(t)$. The elements of these three parameters are defined by

$$\begin{aligned} p_0(X_k) &= \Pr\{X(0) = X_k\}, \\ P_{\text{up}}(X_k, X_h) &= \lim_{t \to \infty} Q(X_k, X_h, t), \\ \mu(X_k) &= \int_0^\infty (1 - \sum_{X_l \in S_{\text{R}}} Q(X_k, X_l, t)) t dt, \end{aligned}$$

where $X_k, X_h \in S_{\text{R}}$, and both are up states. If $I - P_{\text{up}}$ is not invertible, MTTF $= \infty$, which is generally not achievable in practice. In the sequel, $I - P_{\text{up}}$ is assumed to be invertible.

Owing to the construction of $X^{\text{R}}(t)$, it is difficult to establish the analytical relation between controller and MTTF. Considering that MTTF is calculated from the parameters

of X which is constructed based on control performance characteristics γ_{ij}, γ_{ij} can be used as a connection parameter between controller and MTTF. Based on (4.6), the derivative of MTTF with respect to γ_{ij} can be calculated by

$$\frac{d\text{MTTF}}{d\gamma_{ij}} = p_0^T(I - P_{\text{up}})^{-1}\frac{dP_{\text{up}}}{d\gamma_{ij}}(I - P_{\text{up}})^{-1}\mu + p_0^T(I - P_{\text{up}})^{-1}\frac{d\mu}{d\gamma_{ij}}. \tag{4.7}$$

In the set of controllers $\mathbf{K} = \{K_j,\ j \in S_2\}$ or $\mathcal{K} = \{(K_j, L_j), j \in S_2\}$, each K_j or (K_j, L_j) is designed for N_1+1 regime models and therefore determines N_1+1 probabilistic performance parameters γ_{ij}, $i = 0, \cdots, N_1$. For K_j or (K_j, L_j), define the gradient of MTTF as

$$\nabla\text{MTTF}_j \triangleq \frac{[\frac{d\text{MTTF}}{d\gamma_{0j}} \ \cdots \ \frac{d\text{MTTF}}{d\gamma_{N_1 j}}]^T}{\sqrt{\sum_{i\in S_1}(\frac{d\text{MTTF}}{d\gamma_{ij}})^2}}, \tag{4.8}$$

which is composed of the derivatives of MTTF with respect to probabilistic parameters related to K_j or (K_j, L_j), $i \in S_1$, $j \in S_2$. With ∇MTTF_j available, the following gradient-based iterative search algorithm is adopted for MTTF optimization, where $\mathbf{K}^l \triangleq \left\{K_j^l,\ j \in S_2\right\}$ and $\mathcal{K}^l \triangleq \left\{(K_j^l, L_j^l),\ j \in S_2\right\}$ represent the state feedback and 2DOF controllers respectively at the l-th iteration.

Algorithm 4.1: MTTF optimization

1. Initialization: Set $l = 0$; select minimum reliability requirement $\overline{\text{MTTF}}$ and step size $\tau > 0$; randomly generate the initial value of controller $\mathbf{K}^0$ or $\mathcal{K}^0$; and estimate probabilistic performance γ_{ij}^0 using (4.5).

2. At iteration l, calculate MTTF based on controller $\mathbf{K}^l$ or $\mathcal{K}^l$. If MTTF $> \overline{\text{MTTF}}$, stop and the controller at current iteration satisfies MTTF requirement; otherwise, if $\sqrt{\sum_{i\in S_1}(\frac{d\text{MTTF}}{d\gamma_{ij}})^2} < \epsilon$, a small positive number, stop because the algorithm is at a local optimum but $\overline{\text{MTTF}}$ is not achieved.

3. For each $j \in S_2$, calculate ∇MTTF_j^l using (4.7)-(4.8); use Algorithm 4.2 to obtain $\mathbf{K}^{l+1}$ or $\mathcal{K}^{l+1}$ such that $\gamma_{ij}^{l+1} \geq \gamma_{ij}^l + \tau\nabla\text{MTTF}_{ij}^l$ for any $i \in S_1$ and $j \in S_2$, where ∇MTTF_{ij}^l denotes the element of ∇MTTF_j^l.

4. Go to step 2 and start the new iteration $l + 1$.

Remark 4.4 *In Algorithm 4.1, γ_{ij} is iterated along the gradient direction of MTTF, and its value is used to direct controller update. Because the convexity of MTTF with respect to γ_{ij} is not guaranteed, the gradient search may run into a local optimum, and a controller for the required MTTF cannot be found. This problem always exists when using gradient search*

for a non-convex problem. It can be handled by the change of initial values or the relaxation of $\overline{MTTF}$. In step 3, the controller is designed to satisfy the probabilistic performance using Algorithm 4.2 presented in the next section.

4.3 Sequential randomized algorithms for state feedback control

This section considers the design of a state feedback controller. For notational simplicity, for $\zeta(t) = i$, $\eta(t) = j$, $i \in S_1$, $j \in S_2$, denote $A_i(\Delta) \triangleq A(\zeta(t), \Delta)$, $B_i(\Delta) \triangleq B(\zeta(t), \Delta)$, $C_i(\Delta) \triangleq C(\zeta(t), \Delta)$, $D_i(\Delta) \triangleq D(\zeta(t), \Delta)$, $E_i(\Delta) \triangleq E(\zeta(t), \Delta)$, $F_i(\Delta) \triangleq F(\zeta(t), \Delta)$, $\overline{A}_{ij}(\Delta) \triangleq A(\zeta(t), \Delta) + B(\zeta(t), \Delta)K_j$, and $\overline{C}_{ij}(\Delta) \triangleq C(\zeta(t), \Delta) + D(\zeta(t), \Delta)K_j$. For fixed $\zeta(t) = i$ and $\eta(t) = j$, (4.2) is reduced to a linear uncertain system

$$G_{ij}: \begin{cases} \dot{x}(t) = \overline{A}_{ij}(\Delta)x(t) + E_i(\Delta)w(t), \\ z(t) = \overline{C}_{ij}(\Delta)x(t) + F_i(\Delta)w(t). \end{cases} \tag{4.9}$$

Let $G_{ij}(s, \Delta)$ denote the transfer function from $w(t)$ to $z(t)$. Its $\mathcal{H}_\infty$ norm $\|G_{ij}(s, \Delta)\|_\infty$ is selected as the performance criterion, and the probabilistic performance is reduced to $\gamma_{ij} = \Pr\{\|G_{ij}(s, \Delta)\|_\infty \leq \rho_i\}$. The following lemma then provides a sufficient condition to check whether $\|G_{ij}(s, \Delta)\|_\infty \leq \rho_i$. In the sequel, Δ is not shown in system matrices for notational simplicity.

Lemma 4.1 *For system (4.9), assume that the initial state $x(0) = 0$ and $\rho_i^2 I - F_i^T F_i > 0$, where I denotes an identity matrix with compatible dimensions. For fixed i, j, and a particular uncertainty sample Δ, $\|G_{ij}(s)\|_\infty \leq \rho_i$ holds if there exists $P_{ij} \geq 0$ such that*

$$(\overline{A}_{ij})^T P_{ij} + P_{ij}\overline{A}_{ij} + (\overline{C}_{ij})^T \overline{C}_{ij} + (P_{ij}E_i + (\overline{C}_{ij})^T F_i)(\rho_i^2 I - F_i^T F_i)^{-1}(E_i^T P_{ij} + F_i^T \overline{C}_{ij}) \leq 0. \tag{4.10}$$

The proof is standard by using a quadratic Lyapunov function [84, p. 212], and a proof is provided here for clarity.

Proof: For system in (4.9), it is worthwhile to point out that the result to be proved is for fixed i, j, and uncertainty sample Δ. In other words, the result is for a fixed linear regime system in FTCS's.

Suppose that the solution $P_{ij} \geq 0$ exists for (4.10). Using Schur's complement lemma and the assumption that $\rho_i I - F_i^T F_i > 0$, (4.10) is equivalent to

$$\begin{bmatrix} (\overline{A}_{ij})^T P_{ij} + P_{ij}\overline{A}_{ij} + (\overline{C}_{ij})^T \overline{C}_{ij} & P_{ij}E_i + (\overline{C}_{ij})^T F_i \\ E_i^T P_{ij} + F_i^T \overline{C}_{ij} & -(\rho_i^2 I - F_i^T F_i) \end{bmatrix} \leq 0.$$

So, for all $x(t) \in R^n, w(t) \in R^q$,

$$\begin{bmatrix} x(t) \\ w(t) \end{bmatrix}^T \begin{bmatrix} (\overline{A}_{ij})^T P_{ij} + P_{ij}\overline{A}_{ij} + (\overline{C}_{ij})^T \overline{C}_{ij} & P_{ij}E_i + (\overline{C}_{ij})^T F_i \\ E_i^T P_{ij} + F_i^T \overline{C}_{ij} & -(\rho_i^2 I - F_i^T F_i) \end{bmatrix} \begin{bmatrix} x(t) \\ w(t) \end{bmatrix} \leq 0. \quad (4.11)$$

For notational simplicity, let us drop the time variable t in $x(t)$ and $w(t)$. Inequality (4.11) is obviously equivalent to

$$x^T[(\overline{A}_{ij})^T P_{ij} + P_{ij}\overline{A}_{ij} + (\overline{C}_{ij})^T \overline{C}_{ij}]x + x^T[P_{ij}E_i + (\overline{C}_{ij})^T F_i]w + w^T(E_i^T P_{ij} + F_i^T \overline{C}_{ij})x - w^T(\rho_i^2 I - F_i^T F_i)w \leq 0. \quad (4.12)$$

Consider a Lyapunov function $f_{ij}(x) = x^T P_{ij} x$, and $f_{ij}(x) \geq 0$ as $P_{ij} \geq 0$. Using the state equation in (4.9), the derivative of $f_{ij}(x)$ is calculated as

$$\frac{df_{ij}(x)}{dt} = x^T(\overline{A}_{ij}^T P_{ij} + P_{ij}\overline{A}_{ij})x + x^T P_{ij}E_i w + w^T E_i^T P_{ij} x. \quad (4.13)$$

By substituting (4.13) into (4.12), we have

$$\frac{df_{ij}(x)}{dt} \leq \rho_i^2 w^T w - (\overline{C}_{ij}x + F_i w)^T(\overline{C}_{ij}x + F_i w) = \rho_i^2 w^T w - z^T z.$$

Taking integration on both sides from 0 to t_0, we have

$$f_{ij}(x(t_0)) - f_{ij}(x(0)) = \int_0^{t_0} \frac{df_{ij}(x(t))}{dt} dt \leq \int_0^{t_0} (\rho_i^2 w(t)^T w(t) - z(t)^T z(t)) dt.$$

Using $f_{ij}(x(t_0)) \geq 0$ and $f_{ij}(x(0)) = 0$, we obtain

$$\int_0^{t_0} z(t)^T z(t) dt \leq \rho_i^2 \int_0^{t_0} w(t)^T w(t) dt. \quad (4.14)$$

If $w(t)$ has finite L_2-norm, (4.14) yields $\|G_{ij}(s)\|_\infty \leq \rho_i$ by taking the limit as $t_0 \to \infty$.

■

Owing to Lemma 4.1, if inequality (4.10) holds with probability γ_{ij} when Δ varies probabilistically, K_j satisfies probabilistic performance $\gamma_{ij} = \Pr\{\|G_{ij}(s, \Delta)\|_\infty \leq \rho_i\}$. K_j can be designed using a sequential randomized algorithm presented in this section.

The following notations are adopted in this section: The space of real n-by-m matrices is a Hilbert space with the inner product $\langle M, N \rangle \triangleq \text{Tr}(M^T N)$ and Frobenius norm $\|M\| \triangleq \sqrt{\sum_{i=1}^n \sum_{j=1}^m (M(i,j))^2}$, where Tr$(\cdot)$ denotes the trace of a matrix, and m, n the dimensions of M. For a real symmetric matrix M, its projection onto the convex cone of nonnegative definite matrices is defined as

$$M^+ \triangleq \arg\min_{N \geq 0} \|M - N\|.$$

M^+ can be computed explicitly as follows [48]: If $M = U\Lambda U^T$, where U is orthogonal and Λ is diagonal with entries $\lambda_1, \cdots, \lambda_n$, then $M^+ = U\Lambda^+ U^T$, where Λ^+ is diagonal with entries $\max\{0, \lambda_1\}, \cdots, \max\{0, \lambda_n\}$.

4.3.1 Violation function and gradient computation

In this subsection, the matrix inequality (4.10) in Lemma 4.1 is converted to a scalar convex function. Let us begin with a special case that $D_i = F_i = 0$, and the left-hand side of (4.10) is simplified and denoted as V_{ij}, $i \in S_1$, $j \in S_2$:

$$V_{ij} \triangleq A_i^T P_{ij} + P_{ij} A_i + K_j^T B_i^T P_{ij} + P_{ij} B_i K_j + P_{ij} E_i E_i^T P_{ij}/\rho_i^2 + C_i^T C_i \leq 0. \quad (4.15)$$

Let f denote a functional on the space of symmetric matrices which assigns matrix M a real number $f(M)$. The gradient of $f(M)$ is denoted as $\partial_R f(M)$, meaning

$$f(M + \delta M) = f(M) + \langle \partial_M f(M), \delta M \rangle + o(\|\delta M\|),$$

where δM denotes a small perturbation in M. $f(M)$ is convex if and only if [85, p. 69, chap. 3]

$$f(M + \delta M) \geq f(M) + \langle \partial_M f(M), \delta M \rangle.$$

Lemma 4.2 ([79]) *The functional $f(M) \triangleq \frac{1}{2}\|M^+\|^2$ is convex and differentiable with gradient given by $\partial_M f(M) = M^+$.*

Using Lemma 4.2, a violation function of (4.15) is defined as

$$\begin{aligned} v_{ij}(K_j, P_{ij}, \Delta) \triangleq f(V_{ij}) &= \frac{1}{2}\|(A_i^T P_{ij} + P_{ij} A_i + K_j^T B_i^T P_{ij} + P_{ij} B_i K_j \\ &\quad + P_{ij} E_i E_i^T P_{ij}/\rho_i^2 + C_i^T C_i)^+\|^2, \end{aligned} \quad (4.16)$$

where $i \in S_1$ and $j \in S_2$. Obviously, $v_{ij}(K_j, P_{ij}, \Delta) \geq 0$, and $v_{ij}(K_j, P_{ij}, \Delta) = 0$ if and only if $V_{ij} \leq 0$. In other words, (4.15) holds if and only if $v_{ij}(K_j, P_{ij}, \Delta) = 0$.

Lemma 4.3 *$v_{ij}(K_j, P_{ij}, \Delta)$ is convex in K_j and P_{ij} respectively, and its gradients with respect to these two matrix variables are*

$$\begin{aligned} \partial_{K_j} v_{ij}(K_j, P_{ij}, \Delta) &= 2B_i^T P_{ij} V_{ij}^+, \\ \partial_{P_{ij}} v_{ij}(K_j, P_{ij}, \Delta) &= (B_i K_j + A_i + E_i E_i^T P_{ij}/\rho_i^2) V_{ij}^+ + V_{ij}^+ (K_j^T B_i^T + A_i^T \\ &\quad + P_{ij} E_i E_i^T/\rho_i^2). \end{aligned}$$

Proof: Recalling (4.16), because $f(V_{ij})$ is convex in V_{ij}, and V_{ij} is affine in K_j, $v_{ij}(K_j, P_{ij}, \Delta)$ is convex in K_j [85, chap. 4]. The convexity in P_{ij} will be proved after calculating the gradients.

Let δK_j denote a small perturbation in K_j, and the function value after applying this perturbation is calculated as follows, where V_{ij} denotes the expression in (4.15) without any perturbations:

$$\begin{aligned} & v_{ij}(K_j + \delta K_j, P_{ij}, \Delta) \\ = \; & f(V_{ij}) + \langle \partial_{V_{ij}} f(V_{ij}),\ (\delta K_j)^T B_i^T P_{ij} + P_{ij} B_i \delta K_j \rangle + o(\|\delta K_j\|) \\ = \; & v_{ij}(K_j, P_{ij}, \Delta) + \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij})(\delta K_j)^T B_i^T P_{ij}] + \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij}) P_{ij} B_i \delta K_j] \\ & + o(\|\delta K_j\|) \end{aligned} \tag{4.17}$$

Considering that

$$\begin{aligned} \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij})(\delta K_j)^T B_i^T P_{ij}] &= \mathrm{Tr}[(\delta K_j)^T B_i^T P_{ij} \partial_{V_{ij}} f(V_{ij})] \\ &= \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij}) P_{ij} B_i \delta K_j], \end{aligned} \tag{4.18}$$

where we have used the facts that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, $\mathrm{Tr}(A) = \mathrm{Tr}(A^T)$, and the symmetry of P_{ij} and $\partial_{V_{ij}} f(V_{ij})$. By substituting (4.18) into (4.17), we have

$$\begin{aligned} v_{ij}(K_j + \delta K_j, P_{ij}, \Delta) &= v_{ij}(K_j, P_{ij}, \Delta) + 2\mathrm{Tr}[\partial_{V_{ij}} f(V_{ij}) P_{ij} B_i \delta K_j] + o(\|\delta K_j\|) \\ &= v_{ij}(K_j, P_{ij}, \Delta) + \langle 2B_i^T P_{ij} \partial_{V_{ij}} f(V_{ij}),\ \delta K_j \rangle + o(\|\delta K_j\|). \end{aligned}$$

Therefore, $\partial_{K_j} v_{ij}(K_j, P_{ij}, \Delta) = 2B_i^T P_{ij} \partial_{V_{ij}} f(V_{ij}) = 2B_i^T P_{ij} V_{ij}^+$. The gradient with respect to P_{ij} can be proved in a similar way as follows:

$$\begin{aligned} & v_{ij}(K_j, P_{ij} + \delta P_{ij}, \Delta) \\ = \; & f(V_{ij}) + \langle \partial_{V_{ij}} f(V_{ij}),\ A_i^T \delta P_{ij} + \delta P_{ij} A_i + K_j^T B_i^T \delta P_{ij} + \delta P_{ij} B_i K_j + \\ & \delta P_{ij} E_i E_i^T P_{ij}/\rho_i^2 + P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2 \rangle + o(\|\delta P_{ij}\|) \\ = \; & v_{ij}(K_j, P_{ij}, \Delta) + \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij})(A_i^T + K_j^T B_i^T + P_{ij} E_i E_i^T/\rho_i^2)\delta P_{ij}] \\ & + \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij}) \delta P_{ij}(A_i + B_i K_j + E_i E_i^T P_{ij}/\rho_i^2)] + o(\|\delta P_{ij}\|) \\ = \; & v_{ij}(K_j, P_{ij}, \Delta) + \mathrm{Tr}[\partial_{V_{ij}} f(V_{ij})(A_i^T + K_j^T B_i^T + E_i E_i^T/\rho_i^2)\delta P_{ij}] \\ & + \mathrm{Tr}[(A_i + B_i K_j + E_i E_i^T/\rho_i^2)\partial_{V_{ij}} f(V_{ij}) \delta P_{ij}] + o(\|\delta P_{ij}\|) \\ = \; & v_{ij}(K_j, P_{ij}, \Delta) + \langle (B_i K_j + A_i + E_i E_i^T P_{ij}/\rho_i^2) V_{ij}^+ \\ & + V_{ij}^+ (K_j^T B_i^T + A_i^T + P_{ij} E_i E_i^T/\rho_i^2),\ \delta P_{ij} \rangle + o(\|\delta P_{ij}\|). \end{aligned}$$

This proves the gradient in P_{ij}. The convexity in P_{ij} can be shown by the following in-

equality:

$$\begin{aligned} v_{ij}(K_j, P_{ij} + \delta P_{ij}, \Delta) &\geq f(V_{ij}) + \langle \partial_{V_{ij}} f(V_{ij}), A_i^T \delta P_{ij} + \delta P_{ij} A_i + K_j^T B_i^T \delta P_{ij} \\ &\quad + \delta P_{ij} B_i K_j + \delta P_{ij} E_i E_i^T P_{ij}/\rho_i^2 + P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2 \\ &\quad + \delta P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2 \rangle \qquad (4.19) \\ &= v_{ij}(K_j, P_{ij}, \Delta) + \langle \partial_{P_{ij}} v_{ij}(K_j, P_{ij}, \Delta), \ \delta P_{ij} \rangle \\ &\quad + \langle \partial_{V_{ij}} f(V_{ij}), \ \delta P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2 \rangle \qquad (4.20) \\ &\geq v_{ij}(K_j, P_{ij}, \Delta) + \langle \partial_{P_{ij}} v_{ij}(K_j, P_{ij}, \Delta), \ \delta P_{ij} \rangle. \qquad (4.21) \end{aligned}$$

(4.19) is because of the convexity of f, (4.20) follows by substituting $\partial_{P_{ij}} v_{ij}(K_j, P_{ij}, \Delta)$ in (4.19), and (4.21) is true because that $\mathrm{Tr}[\partial_{V_{ij}} f(V_{ij}) \delta P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2] \geq 0$, resulted from the semi-definite properties of $\partial_{V_{ij}} f(V_{ij})$ and $\delta P_{ij} E_i E_i^T \delta P_{ij}/\rho_i^2$. ■

For the general cases that $D_i \neq 0$ and $F_i \neq 0$, the gradients are given as follows, which can be proved in a similar way:

$$\begin{aligned} \partial_{K_j} v_{ij}(K_j, P_{ij}, \Delta) &= 2[B_i^T P_{ij} + D_i^T C_i + D_i^T F_i(\rho_i^2 I - F_i^T F_i)^{-1} E_i^T P_{ij}^T \\ &\quad + (D_i^T D_i + D_i^T F_i(\rho_i^2 I - F_i^T F_i)^{-1} F_i^T D_i) K_j] V_{ij}^+, \\ \partial_{P_{ij}} v_{ij}(K_j, P_{ij}, \Delta) &= [A_i + B_i K_j + E_i(\rho_i^2 I - F_i^T F_i)^{-1} F_i^T (C_i + D_i K_j) + E_i \\ &\quad (\rho_i^2 I - F_i^T F_i)^{-1} E_i^T] V_{ij}^+ + V_{ij}^+ [A_i^T + K_j^T B_i + (C_i + D_i K_j)^T \\ &\quad F_i(\rho_i^2 I - F_i^T F_i)^{-1} E_i + E_i(\rho_i^2 I - F_i^T F_i)^{-1} E_i^T]. \end{aligned}$$

Owing to false alarms, the FDI estimate $\eta(t)$ may be different from $\zeta(t)$. As a result, given fixed $j \in S_2$, each controller gain K_j may appear in $N_1 + 1$ inequalities, $V_{ij} \leq 0$ for $i = 0, 1, \cdots, N_1$. To take these $N_1 + 1$ inequalities into account simultaneously, a weighted composite violation function is defined as

$$\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = \sum_{i=0}^{N_1} \theta_{ij} v_{ij}(K_j, P_{ij}, \Delta), \qquad (4.22)$$

where θ_{ij} denotes a positive weight corresponding to inequality $V_{ij} \geq 0$ for $\zeta(t) = i$, $i \in S_1, j \in S_2$.

Lemma 4.4 *Given $j \in S_2$, if $\theta_{ij} > 0$ for all $i \in S_1$, $\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}) = 0$ is equivalent to $V_{ij} \leq 0$ simultaneously for all $i \in S_1$.*

Proof: As $\theta_{ij} > 0$ and $v_{ij}(K_j, P_{ij}, \Delta) \geq 0$, $\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = 0$ if and only if $v_{ij} = 0$ holds simultaneously for $i = 0, 1, \cdots, N_1, j \in S_2$. Based on the definition of v_{ij} in (4.16), $v_{ij}(K_j, P_{ij}, \Delta) = 0$ if and only if $V_{ij} \leq 0$, which concludes the proof. ■

Lemma 4.4 shows that ψ_j can be used as a composite violation function for multiple matrix inequalities if all weights are positive. So, θ_{ij} can be selected freely among all positive values.

Lemma 4.5 *Given $j \in S_2$, $\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j})$ is convex in K_j and P_{ij}, $i \in S_1$, and its gradients are given by*

$$\partial_{K_j}\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = \sum_{i=0}^{N_1} \theta_{ij}\partial_{K_j} v_{ij}(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta), \quad (4.23)$$

$$\partial_{P_{ij}}\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = \theta_{ij}\partial_{P_{ij}} v_{ij}(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta). \quad (4.24)$$

Lemma 4.5 is obvious considering (4.22) and the properties of gradient and convexity.

4.3.2 Controller design algorithm

Let S^j_{KP} represents the robust solution set of (4.22) defined as

$$S^j_{KP} \triangleq \{(K_j, P_{0j}, P_{1j}, \cdots, P_{N_1 j}) : \psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = 0,\ \forall \Delta \in \Omega\}. \quad (4.25)$$

Two standard assumptions of sequential algorithms are made here as follows [48]:

Assumption 4.1 *The solution set S^j_{KP} defined in (4.25) contains a nonempty interior for any given $j \in S_2$.*

Assumption 4.2 *If $(K_j, P_{0j}, P_{1j}, \cdots, P_{N_1 j}) \notin S_{KP}$, $\Pr\{\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) > 0\} > 0$.*

Based on Assumption 4.1, there exists an interior point $(K_j^{\#}, P_{0j}^{\#}, \cdots, P_{N_1 j}^{\#}) \in S^j_{KP}$ and a ball $B_{r_j} \subset S^j_{KP}$centered at $(K_j^{\#}, P_{0j}^{\#}, \cdots, P_{N_1 j}^{\#})$. The knowledge of radius r_j of B_{r_j} can be used to determine step size in the algorithm presented in this section.

In Algorithm 4.1, the control design algorithm is to find $(K_j^{l+1}, P_{0j}^{l+1}, \cdots P_{N_1 j}^{l+1})$ such that $\gamma_{ij}^{l+1} \geq \gamma_{ij}^{l} + \tau\nabla\text{MTTF}_{ij}^{l}$, where $i \in S_1$, $j \in S_2$, and $l \in \mathbb{N}$ represents the iteration index of Algorithm 4.1. The algorithm is in an iterative structure: At iteration $k \in \mathbb{N}$, if the violation function $\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k) > 0$ for a randomly generated uncertainty sample Δ^k, K_j^{k+1} and P_{ij}^{k+1} are updated by

$$K_j^{k+1} = K_j^k - \mu_j^k \frac{\partial_{K_j}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}, \quad (4.26)$$

$$P_{ij}^{k+1} = [P_{ij}^k - \mu_j^k \frac{\partial_{P_{ij}}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}]^+, \quad (4.27)$$

where ϕ_j represents the overall size of the gradient in Lemma 4.5:

$$\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k) \triangleq (\|\partial_{K_j}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)\|^2 + \sum_{i=0}^{N_1} \|\partial_{P_{ij}}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)\|^2)^{1/2} \quad (4.28)$$

μ_j^k denotes the step-size calculated by

$$\mu_j^k \triangleq \frac{\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)} + r_j, \quad (4.29)$$

where $r_j > 0$ denotes the radius of $B_{r_j} \subset S_{KP}$ centered at $(K_j^\#, P_{0j}^\#, \cdots, P_{N_1 j}^\#)$.

Remark 4.5 *In this paper, r_j is assumed to be a known priori for choosing step size μ_j^k in the sequential algorithm. If r_j is not known, classical choice of step size in stochastic gradient algorithms can be used for μ_j^k. For example, $\lim_{k\to\infty}\mu_j^k = 0$ and $\sum_{k=0}^{\infty}\mu_j^k = \infty$ [78, 86].* Note that the projection operation is used in (4.27) to ensure P_{ij} converge to a nonnegative definite matrix. If the violation function $\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k) = 0$, let $K_j^{k+1} = K_j^k$ and $P_{ij}^{k+1} = P_{ij}^k$, $i \in S_1, j \in S_2$.

The controller design algorithm is given in Algorithm 4.2, where $\gamma_{ij}^{l\bullet} \triangleq \gamma_{ij}^l + \tau\nabla\text{MTTF}_{ij}^l$, i denotes fault mode, j FDI mode, l iteration index in Algorithm 4.1, and k iteration index in Algorithm 4.2.

Algorithm 4.2 Controller design for probabilistic performance

1. Initialization: Set $k = 0$, $K_j^{l0} = K_j^l$, and $P_{ij}^{l0} = P_{ij}^l$, taken from iteration l in Algorithm 4.1, $i \in S_1, j \in S_2$.

2. At iteration k, estimate the probabilistic performance γ_{ij}^{lk} of K_j^{lk} using (4.5) for all $i \in S_1$. If $\gamma_{ij}^{lk} \geq \gamma_{ij}^{l\bullet}$ for all $i \in S_1$, stop and return K_j^{lk} to Algorithm 4.1 as K_j^{l+1}.

3. Determine positive weight θ_{ij}^{lk} based on γ_{ij}^{lk}, $\gamma_{ij}^{l\bullet}$, and ∇MTTF_{ij}^l, $i \in S_1$.

4. Generate an uncertainty sample Δ^{lk}; if $\psi_j(K_j^{lk}, P_{0j}^{lk}, \cdots, P_{N_1 j}^{lk}, \Delta^{lk}) > 0$, update K_j^{lk} and P_{ij}^{lk} using (4.26) and (4.27) respectively; then, goto step 2.

As the probabilistic performance requirement $\gamma_{ij}^{l\bullet}$ is calculated based on the gradient ∇MTTF_{ij}^l, it is ideal to have γ_{ij}^{lk} increase along this gradient direction for fast convergence. Based on Lemma 4.4, $\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta)$ is a valid composite violation function as long as the weight $\theta_{ij}^{lk} > 0$. Considering that θ_{ij}^{lk} also appear in gradient calculation (4.23)-(4.24), the increasing direction of γ_{ij}^{lk} can be adjusted by determining θ_{ij}^{lk} based on heuristic rules, which helps to reduce iteration number.

4.3.3 Convergence result

Theorem 4.1 *If Assumption 4.1 holds, the iterations (4.26)-(4.27) ensure the following inequality*

$$\left\|K_j^{k+1} - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^{k+1} - P_{ij}^{\#}\right\|^2 \leq \left\|K_j^{k} - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^{k} - P_{ij}^{\#}\right\|^2 - r_j^2, \quad (4.30)$$

where $(K_j^{\#}, P_{0j}^{\#}, \cdots, P_{N_1 j}^{\#}) \in S_{KP}$ *denotes a robust solution.*

Proof: The proof follows standard procedure in subgradient algorithms [48, 78, 79]. Owing to Assumption 4.1, define the following feasible solution in S_{KP}:

$$\overline{K}_j = K_j^{\#} + r_j \frac{\partial_{K_j}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}, \quad (4.31)$$

$$\overline{P}_{ij} = P_{ij}^{\#} + r_j \frac{\partial_{P_{ij}}\psi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}, \ i \in S_1. \quad (4.32)$$

So, $\psi_j(\overline{K}_j, \overline{P}_{0j}, \cdots, \overline{P}_{N_1 j}, \Delta) = 0$ for all $\Delta \in \Omega$. For notational simplicity, the variables of ψ_j are omitted. If $\psi_j > 0$, we have

$$\begin{aligned}
&\left\|K_j^{k+1} - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^{k+1} - P_{ij}^{\#}\right\|^2 \\
&= \left\|K_j^k - K_j^{\#} - \mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j}\right\|^2 + \sum_{i=0}^{N_1} \left\|[P_{ij}^k - \mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j}]^+ - P_{ij}^{\#}\right\|^2 \\
&\leq \left\|K_j^k - K_j^{\#} - \mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j}\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^k - \mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j} - P_{ij}^{\#}\right\|^2 \\
&= \left\|K_j^k - K_j^{\#}\right\|^2 - 2\mu_j^k \langle \frac{\partial_{K_j}\psi_j}{\phi_j}, K_j^k - \overline{K}_j\rangle - 2\mu_j^k \langle \frac{\partial_{K_j}\psi_j}{\phi_j}, \overline{K}_j - K_j^{\#}\rangle + \left\|\mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j}\right\|^2 \\
&\quad + \sum_{i=0}^{N_1} (\left\|P_{ij}^k - P_{ij}^{\#}\right\|^2 - 2\mu_j^k \langle \frac{\partial_{P_{ij}}\psi_j}{\phi_j}, P_{ij}^k - \overline{P}_{ij}\rangle - 2\mu_j^k \langle \frac{\partial_{P_{ij}}\psi_j}{\phi_j}, \overline{P}_{ij} - P_{ij}^{\#}\rangle \\
&\quad + \left\|\mu_j^k \frac{\partial_{P_{ij}}\psi_j}{\phi_j}\right\|^2),
\end{aligned}$$

where the inequality is because of the property of projection operation [48]. Based on (4.28), we have

$$\left\|\mu_j^k \frac{\partial_{K_j}\psi_j}{\phi_j}\right\|^2 + \sum_{i=0}^{N_1} \left\|\mu_j^k \frac{\partial_{P_{ij}}\psi_j}{\phi_j}\right\|^2 = (\mu_j^k)^2.$$

Owing to the convexity of ψ_j in K_j and P_{ij}, we have

$$\langle \frac{\partial_{K_j}\psi_j}{\phi_j},\ K_j^k - \overline{K}_j\rangle \geq \frac{\psi_j}{\phi_j},\ \langle \frac{\partial_{P_{ij}}\psi_j}{\phi_j},\ P_{ij}^k - \overline{P}_{ij}\rangle \geq \frac{\psi_j}{\phi_j}.$$

Because of (4.28) and (4.31)-(4.32), we have

$$\langle \frac{\partial_{K_j}\psi_j}{\phi_j},\ \overline{K}_j - K_j^{\#}\rangle + \sum_{i=0}^{N_1}\langle \frac{\partial_{P_{ij}}\psi_j}{\phi_j},\ \overline{P}_{ij} - P_{ij}^{\#}\rangle = r_j.$$

Therefore, we have

$$\begin{aligned}\left\|K_j^{k+1} - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1}\left\|P_{ij}^{k+1} - P_{ij}^{\#}\right\|^2 \ \leq\ & \left\|K_j^k - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1}\left\|P_{ij}^k - P_{ij}^{\#}\right\|^2 + (\mu_j^k)^2 \\ & -2\mu_j^k(\frac{\psi_j}{\phi_j} + r_j).\end{aligned}$$

By substituting μ_j^k defined in (4.29), we have

$$\left\|K_j^{k+1} - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1}\left\|P_{ij}^{k+1} - P_{ij}^{\#}\right\|^2 \leq \left\|K_j^k - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1}\left\|P_{ij}^k - P_{ij}^{\#}\right\|^2 - (\frac{\psi_j}{\phi_j} + r_j)^2.$$

$$\leq \left\|K_j^k - K_j^{\#}\right\|^2 + \sum_{i=0}^{N_1}\left\|P_{ij}^k - P_{ij}^{\#}\right\|^2 - r_j^2.$$

So, (4.30) holds, meaning that the distance to the robust solution is decreasing monotonically. ■

Remark 4.6 *The iterations (4.26)-(4.27) are originated from subgradient methods, and their convergence is usually proved based on the distance between the decision variables and the solution set [86, p. 25]. Theorem 4.1 also follows this idea: after each iteration, the distance of controller to robust solution set is reduced by at least τ_j^2. So only finite updates are needed before reaching the solution set. Considering there is a positive probability of performing the update based on Assumption 4.2, this theorem leads to the following convergence result of Algorithm 4.2.*

Proposition 4.1 *If Assumptions 4.1 and 4.2 hold, Algorithm 4.2 converges in a finite number of iterations with probability 1 to a controller satisfying required probabilistic performance.*

Proof: Considering Assumption 4.2, there is a positive probability of generating an uncertainty sample with $\psi_j(K_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) > 0$ and performing the iteration (4.26)-(4.27) when $(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k) \notin S_{KP}$. In other words, the distance of $(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k)$

to S_{KP} decreases by at least r_j^2 with a positive probability when $(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k) \notin S_{KP}$. Therefore, $(K_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k)$ converges to a robust solution in S_{KP} in a finite number of iterations with probability one, which implies the convergence to a controller with any probabilistic performance. ■

4.4 Sequential randomized algorithms for 2DOF control

The design of 2DOF control parallels that of state feedback control. For fixed regime modes $\zeta(t) = i$ and $\eta(t) = j$, $i \in S_1$, $j \in S_2$, the closed-loop system (4.3) is reduced to a linear uncertain system

$$G_{ij}: \begin{cases} \dot{x}(t) = \overline{A}_{ij}x(t) + (E_i + B_i L_j)w(t), \\ z(t) = \overline{C}_{ij}x(t) + (F_i + D_i L_j)w(t), \end{cases} \tag{4.33}$$

where the simplified notations in Section 4.3 have been used. Following Lemma 4.1, its $\mathcal{H}_\infty$ norm is non-greater than ρ_i if there exists $P_{ij} > 0$ such that

$$\overline{A}_{ij}^T P_{ij} + P_{ij}\overline{A}_{ij} + \overline{C}_{ij}^T \overline{C}_{ij} + [P_{ij}(E_i + B_i L_j) + \overline{C}_{ij}^T (F_i + D_i L_j)]$$
$$[\rho_i^2 I - (F_i + D_i L_j)^T (F_i + D_i L_j)]^{-1} [(E_i + B_i L_j)^T P_{ij} + (F_i + D_i L_j)^T \overline{C}_{ij}] \le 0. \tag{4.34}$$

As the controller gain L_j is involved with matrix inverse in this inequality, its convexity is violated when $D_i \neq 0$. So $D_i = 0$ is assumed in order to apply sequential randomized algorithms. Let us begin with the case that $F_i = 0$, and the matrix inequality is reduced to

$$\begin{aligned} W_{ij} \triangleq\ & A_i^T P_{ij} + P_{ij} A_i + K_j^T B_i^T P_{ij} + P_{ij} B_i K_j \\ & + P_{ij}(E_i + B_i L_j)(E_i + B_i L_j)^T P_{ij}/\rho_i^2 + C_i^T C_i \le 0. \end{aligned} \tag{4.35}$$

A violation function of (4.35) can be defined as

$$\begin{aligned} w_{ij}(K_j, L_j, P_{ij}, \Delta) \triangleq\ & f(W_{ij}) = \frac{1}{2}\|(A_i^T P_{ij} + P_{ij} A_i + K_j^T B_i^T P_{ij} + P_{ij} B_i K_j \\ & + P_{ij}(E_i + B_i L_j)(E_i + B_i L_j)^T P_{ij}/\rho_i^2 + C_i^T C_i)^+\|^2. \end{aligned} \tag{4.36}$$

Lemma 4.6 *$w_{ij}(K_j, L_j, P_{ij}, \Delta)$ is convex in K_j, L_j, and P_{ij} respectively, and its gradients with respect to these matrix variables are*

$$\begin{aligned} \partial_{K_j} w_{ij}(K_j, L_j, P_{ij}, \Delta) &= 2B_i^T P_{ij} W_{ij}^+, \\ \partial_{L_j} w_{ij}(K_j, L_j, P_{ij}, \Delta) &= 2B_i^T P_{ij} W_{ij}^+ P_{ij}(B_i L_j + E_i), \end{aligned}$$

$$\begin{aligned} \partial_{P_{ij}} w_{ij}(K_j, L_j, P_{ij}, \Delta) =\ & [B_i K_j + A_i + (E_i + B_i L_j)(E_i + B_i L_j)^T P_{ij}/\rho_i^2] W_{ij}^+ \\ & + W_{ij}^+ [K_j^T B_i^T + A_i^T + P_{ij}(E_i + B_i L_j)(E_i + B_i L_j)^T/\rho_i^2]. \end{aligned}$$

Lemma 4.6 can be proved in the same way as Lemma 4.3. This simplified case of $F_i = 0$ corresponds to 2DOF control in model-matching design for transient performance and is of major interest in this chapter, as demonstrated in Section 4.6. The gradients and convexity in the general case of $F_i \neq 0$ can be derived in a similar way and are omitted here for brevity.

Compared with state feedback control in Section 4.3, 2DOF control involves two control gains (K_j, L_j) and therefore one more decision variable. But, the sequential randomized algorithms can be constructed following the same procedures, which are listed as follows without proof. For convenience and comparison purpose, the same notations are used here as in Section 4.3.

The composite violation function is defined as

$$\psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = \sum_{i=0}^{N_1} \theta_{ij} w_{ij}(K_j, L_j, P_{ij}, \Delta), \tag{4.37}$$

and its gradients are

$$\begin{aligned} & \partial_{K_j} \psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) \\ = & \sum_{i=0}^{N_1} \theta_{ij} \partial_{K_j} w_{ij}(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta), \qquad (4.38) \\ & \partial_{L_j} \psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) \\ = & \sum_{i=0}^{N_1} \theta_{ij} \partial_{L_j} w_{ij}(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta), \qquad (4.39) \\ & \partial_{P_{ij}} \psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) \\ = & \theta_{ij} \partial_{P_{ij}} w_{ij}(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta), i = 0 \cdots N_1. \qquad (4.40) \end{aligned}$$

At k-th iteration of randomized algorithm, if the violation function is greater than zero, denoted as $\psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k) > 0$, K_j^{k+1}, L_j^{k+1}, and P_{ij}^{k+1} are updated by

$$K_j^{k+1} = K_j^k - \mu_j^k \frac{\partial_{K_j} \psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}, \tag{4.41}$$

$$L_j^{k+1} = L_j^k - \mu_j^k \frac{\partial_{L_j} \psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}, \tag{4.42}$$

$$P_{ij}^{k+1} = [P_{ij}^k - \mu_j^k \frac{\partial_{P_{ij}} \psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}]^+, \tag{4.43}$$

where $\mu_j^k \triangleq \frac{\psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)}{\phi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)} + r_j$, and

$$\begin{aligned}
&\phi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k) \\
\triangleq\ &(\|\partial_{K_j}\psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)\|^2 + \|\partial_{L_j}\psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)\|^2 \\
&+ \sum_{i=0}^{N_1} \|\partial_{P_{ij}}\psi_j(K_j^k, L_j^k, P_{0j}^k, \cdots, P_{N_1 j}^k, \Delta^k)\|^2)^{1/2}. \qquad (4.44)
\end{aligned}$$

$r_j > 0$ denotes the radius of S_{KLP} centered at $(K_j^\#, L_j^\#, P_{0j}^\#, \cdots, P_{N_1 j}^\#)$, and S_{KLP} represents the robust solution set defined as

$$S_{KLP} \triangleq \{(K_j, L_j, P_{0j}, P_{1j}, \cdots, P_{N_1 j}) : \psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) = 0,\ \forall \Delta \in \Omega\}. \qquad (4.45)$$

If S_{KLP} contains a nonempty interior for any given $j \in S_2$, the iterations (4.41)-(4.43) ensure the following inequality

$$\begin{aligned}
&\left\|K_j^{k+1} - K_j^\#\right\|^2 + \left\|L_j^{k+1} - L_j^\#\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^{k+1} - P_{ij}^\#\right\|^2 \\
\leq\ &\left\|K_j^k - K_j^\#\right\|^2 + \left\|L_j^k - L_j^\#\right\|^2 + \sum_{i=0}^{N_1} \left\|P_{ij}^k - P_{ij}^\#\right\|^2 - r_j^2.
\end{aligned}$$

The inequality (4.46) can be derived in a similar way as in Theorem 4.1, which leads to the convergence of the iterative updates. The 2DOF controller design algorithm can be implemented by replacing the iterations (4.26)-(4.27) with (4.41)-(4.43) in Algorithm 4.2. And it can be used with Algorithm 4.1 to find a 2DOF controller for MTTF optimization. If $(K_j, L_j, P_{0j}, P_{1j}, \cdots, P_{N_1 j}) \notin S_{KLP}$ implies $\Pr\{\psi_j(K_j, L_j, P_{0j}, \cdots, P_{N_1 j}, \Delta) > 0\} > 0$, Algorithm 4.2 with iterations (4.41)-(4.43) is guaranteed to converge to a 2DOF controller satisfying required performance with probability 1, which can be proved similarly as in Proposition 4.1.

Remark 4.7 *Both the state feedback and 2DOF controller require complete information of states and can be designed using sequential randomized algorithms, in which the iterative updates and convergence proof are similar. Their differences lie in the following aspects: 1) The 2DOF design is originated from model-matching problem and needs the knowledge of $w(t)$; 2) it requires the condition $D_j = 0$ to apply the algorithm; 3) it involves one additional feedforward gain L_j, which appears as a new decision variable in the design algorithm.*

4.5 Output feedback control

We consider a general scenario when plant state is not available for controller and the plant output equation is

$$y(t) = U(\zeta(t), \Delta)x(t) + M(\zeta(t), \Delta)u(t) + N(\zeta(t), \Delta)w(t), \tag{4.46}$$

where $y(t) \in \mathbb{R}^l$ represents measured output, and $U(\zeta(t), \Delta)$, $M(\zeta(t), \Delta)$, and $N(\zeta(t), \Delta)$ system matrices. By using $y(t)$ instead of $x(t)$ in the original 2DOF control, the control input becomes

$$\begin{aligned} u(t) &= K_{\eta(t)}y(t) + L_{\eta(t)}w(t) \\ &= K_{\eta(t)}U(\zeta(t), \Delta)x(t) + K_{\eta(t)}M(\zeta(t), \Delta)u(t) \\ &\quad +[K_{\eta(t)}N(\zeta(t), \Delta) + L_{\eta(t)}]w(t). \end{aligned} \tag{4.47}$$

Obviously, closed-loop system is well-posed if and only if $I - K_{\eta(t)}M(\zeta(t), \Delta)$ is non-singular, which leads to

$$u(t) = [I - K_{\eta(t)}M(\zeta(t), \Delta)]^{-1}[K_{\eta(t)}U(\zeta(t), \Delta)x(t) + (K_{\eta(t)}N(\zeta(t), \Delta) + L_{\eta(t)})w(t)].$$

Substitute $u(t)$ into (4.1), and the closed-loop system equation becomes

$$\begin{cases} \dot{x}(t) = [A(\zeta(t), \Delta) + B(\zeta(t), \Delta)(I - K_{\eta(t)}M(\zeta(t), \Delta))^{-1}K_{\eta(t)}U(\zeta(t), \Delta)]x(t) \\ \qquad +[E(\zeta(t), \Delta) + B(\zeta(t), \Delta)(I - K_{\eta(t)}M(\zeta(t), \Delta))^{-1} \\ \qquad (K_{\eta(t)}N(\zeta(t), \Delta) + L_{\eta(t)})]w(t), \\ z(t) = [C(\zeta(t), \Delta) + D(\zeta(t), \Delta)(I - K_{\eta(t)}M(\zeta(t), \Delta))^{-1}K_{\eta(t)}U(\zeta(t), \Delta)]x(t) \\ \qquad +[F(\zeta(t), \Delta) + D(\zeta(t), \Delta)[I - K_{\eta(t)}M(\zeta(t), \Delta)]^{-1} \\ \qquad (K_{\eta(t)}N(\zeta(t), \Delta) + L_{\eta(t)})]w(t). \end{cases}$$

For fixed regime modes $\zeta(t) = i$ and $\eta(t) = j$, $i \in S_1$, $j \in S_2$, the closed-loop system is reduced to a linear uncertain system

$$G_{ij} : \begin{cases} \dot{x}(t) = [A_i + B_i(I - K_jM_i)^{-1}K_jU_i]x(t) + \\ \qquad [E_i + B_i(I - K_jM_i)^{-1}(K_jN_i + L_j)]w(t), \\ z(t) = [C_i + D_i(I - K_jM_i)^{-1}K_jU_i]x(t) + \\ \qquad [F_i + D_i(I - K_jM_i)^{-1}(K_jN_i + L_j)]w(t). \end{cases} \tag{4.48}$$

where the simplified notations in Section 4.3 have been used. Following Lemma 4.1, a matrix inequality can be derived to have $\|G_{ij}(s, \Delta)_\infty\| \leq \rho_i$. However, matrix inverse terms involving controller gains may appear in the inequality and violate convexity. Therefore,

$D_i = 0$ and $M_i = 0$ are assumed in order to apply sequential algorithms, and the inequality is reduced to:

$$\begin{aligned} W_{ij} \triangleq\ & (A_i + B_iK_jU_i)^TP_{ij} + P_{ij}(A_i + B_iK_jU_i) + C_i^TC_i + [P_{ij}(E_i + B_iK_jN_i \\ & + B_iL_i) + C_i^TF_i](\rho_i^2I - F_i^TF_i)^{-1}[(E_i + B_iK_jN_i + B_iL_i)^TP_{ij} + F_i^TC_i]. \end{aligned}$$

Its violation function can be defined as

$$w_{ij}(K_j, L_j, P_{ij}, \Delta) \triangleq \frac{1}{2}\|W_{ij}\|^2. \tag{4.49}$$

Note same notations of violation functions and gradients are used as in Section 4.4 for comparison purpose.

Lemma 4.7 *$w_{ij}(K_j, L_j, P_{ij}, \Delta)$ defined in (4.49) is convex in K_j, L_j, and P_{ij}, and its gradients are*

$$\begin{aligned} \partial_{K_j}W_{ij} &= 2B_i^TP_{ij}W_{ij}^+(P_{ij}E_i + P_{ij}B_iL_j + C_i^TF_i + P_{ij}B_iK_jN_i)(\rho_i^2I - F_i^TF_i)^{-1}N_i^T, \\ \partial_{L_j}W_{ij} &= 2B_i^TP_{ij}W_{ij}^+(P_{ij}B_iL_j + P_{ij}E_i + P_{ij}B_iK_jN_i + C_i^TF_i)(\rho_i^2I - F_i^TF_i)^{-1}, \\ \partial_{P_{ij}}W_{ij} &= [A_i + B_iK_jU_i + (E_i + B_iK_jN_i + B_iL_i)(\rho_i^2I - F_i^TF_i)^{-1}F_i^TC_i \\ &\quad + (E_i + B_iK_jN_i + B_iL_i)(\rho_i^2I - F_i^TF_i)^{-1}(E_i + B_iK_jN_i + B_iL_i)^TP_{ij}]W_{ij}^+ \\ &\quad + W_{ij}^+[A_i^T + U_i^TK_j^TB_i^T + C_i^TF_i(\rho_i^2I - F_i^TF_i)^{-1}(E_i + B_iK_jN_i + B_iL_i)^T \\ &\quad + P_{ij}(E_i + B_iK_jN_i + B_iL_i)(\rho_i^2I - F_i^TF_i)^{-1}(E_i + B_iK_jN_i + B_iL_i)^T], \end{aligned}$$

Lemma 4.7 can be proved in the same way as Lemmas 4.3 and 4.6. Once a convex violation function and its gradients are found, the remaining procedures are similar as (4.37)-(4.44) and omitted here for brevity. Compared with 2DOF control using state feedback, output 2DOF control contains more complicated calculations of gradients. The corresponding output feedback control of Section 4.3 is to use only $y(t)$ for controller design, which can be deemed as a special case by making $L_j = 0$ in (4.47).

4.6 Example

We consider a demonstration example used in [48] which studies the lateral motion of an aircraft. The plant model under fault-free mode is given by

$$\dot{x}_p(t) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & L_p & L_\beta & L_r \\ g/V & 0 & Y_\beta & -1 \\ N_{\dot{\beta}} & N_p & N_\beta + N_{\dot{\beta}}Y_\beta & N_r - N_{\dot{\beta}} \end{bmatrix} x_p(t) + \begin{bmatrix} 0 & 0 \\ 0 & -3.91 \\ 0.035 & 0 \\ -2.53 & 0.31 \end{bmatrix} u(t),$$

where the components in state $x_p(t)$ represent respectively bank angle, directive of bank angle, sideslip angle, and yaw rate. Two control inputs are rudder and aileron deflections respectively. The considered faulty mode is the 50% loss of effectiveness in both actuators, represented by the reduction of control input matrices.

The control objective considered here is to make the side slip angle, the third state of $x_p(t)$, track pilot's command, represented by exogenous input $w(t)$. The desired response model from $w(t)$ to side slip angle is represented by a first-order transfer function $\frac{2}{s+1}$. This is a typical model-matching problem as illustrated in Figure 4.1. Let $x_m(t)$ denote the state of the desired model, and $x(t) \triangleq [x_p^T(t) \;\; x_m(t)]^T$, the augmented state vector. The model-matching problem can be converted to the following standard set-up

$$\begin{aligned}
\dot{x}(t) &= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & L_p & L_\beta & L_r & 0 \\ g/V & 0 & Y_\beta & -1 & 0 \\ N_{\dot\beta} & N_p & N_\beta + N_{\dot\beta} Y_\beta & N_r - N_{\dot\beta} & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} w(t) \\
&\quad + B(\zeta(t)) u(t, \eta(t)), \\
z(t) &= [0 \;\; 0 \;\; -1 \;\; 0 \;\; 2] x(t),
\end{aligned}$$

where $u(t, \eta(t)) = K_{\eta(t)} x(t) + L_{\eta(t)} w(t)$ represents a 2DOF controller in a switching structure. $B(\zeta(t))$ represents the fault effects on control input matrices. Let B_0 and B_1 denote $B(\zeta(t))$ when $\zeta(t)$ is in mode 0 and 1 respectively:

$$B_0 = \begin{bmatrix} 0 & 0 \\ 0 & -3.91 \\ 0.035 & 0 \\ -2.53 & 0.31 \\ 0 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0 & 0 \\ 0 & -1.955 \\ 0.0175 & 0 \\ -1.265 & 0.155 \\ 0 & 0 \end{bmatrix}.$$

The modeling uncertainties are introduced by aircraft parameters, and the random vector $\Delta = [L_p \;\; L_\beta \;\; L_r \;\; g/V \;\; Y_\beta \;\; N_{\dot\beta} \;\; N_p \;\; N_\beta \;\; N_r]^T$. The mean values of these parameters are: $L_p = -2.93$, $L_\beta = -4.75$, $L_r = 0.78$, $g/V = 0.086$, $Y_\beta = -0.11$, $N_{\dot\beta} = 0.1$, $N_p = -0.042$, $N_\beta = 2.601$, and $N_r = -0.29$. Each parameter is assumed to be perturbed by a relative uncertainty of 10%. For example, L_β is bounded in the interval $[-3.223, -2.637]$. The probability distribution of each parameter is assumed to be a uniform distribution within the corresponding interval.

The fault occurrences and FDI mode transitions are characterized by the generator matrices of $\zeta(t)$ and $\eta(t)$:

$$H_\zeta = \begin{bmatrix} -0.005 & 0.005 \\ 0 & 0 \end{bmatrix}, \; H_\eta^0 = \begin{bmatrix} -0.2 & 0.2 \\ 2 & -2 \end{bmatrix}, \; H_\eta^1 = \begin{bmatrix} -2 & 2 \\ 0.2 & -0.2 \end{bmatrix}.$$

These parameters can be interpreted as follows: According to H_ζ, the mean occurrence time of faults is 200 minutes, and the faulty state is absorbing as the components on the second row are all zeros; according to H_η^0, under fault-free mode, the mean time of false alarms is 5 minutes and that of returning time from false alarms is 0.5 minute; according to H_η^1, the mean time of missing detections is 5 minutes and mean returning time is 0.5 minute. So, this FDI may give frequent incorrect detections.

In this standard set-up, the plant state $x_p(t)$ and model state $x_m(t)$ are both incorporated into state dynamics $x(t)$, $w(t)$ represents command input, and $z(t)$ the mismatch error between the plant and desired responses of side slip angle. Under each fixed regime modes $\zeta(t) = i$ and $\eta(t) = j$, the performance measure is selected as the $\mathcal{H}_\infty$ norm of closed-loop transfer function from $w(t)$ to $z(t)$, denoted by $\|G_{ij}(s, \Delta)\|_\infty$. It describes the difference between the plant response and the desired one; when $\|G_{ij}(s, \Delta)\|_\infty$ is small, the plant transient behavior of side slip angle is expected to resemble the desired one. The allowable $\mathcal{H}_\infty$ bound ρ_i is assumed to be 0.5 for $i = 0$ and 0.75 for $i = 1$. So, when $\zeta(t) = 0$, the system is deemed to fail if $\|G_{ij}(s, \Delta)\|_\infty > 0.5$ for a duration over hard deadline $T_{\text{hd}} = 5$ minutes; when $\zeta(t) = 1$, it is deemed to fail if $\|G_{ij}(s, \Delta)\|_\infty > 0.75$ for a duration over hard deadline. Our design objective is to find a 2DOF controller such that the overall MTTF is greater than 100 minutes (Note that frequent incorrect FDI decisions are assumed and this short MTTF design is for demonstration purpose only).

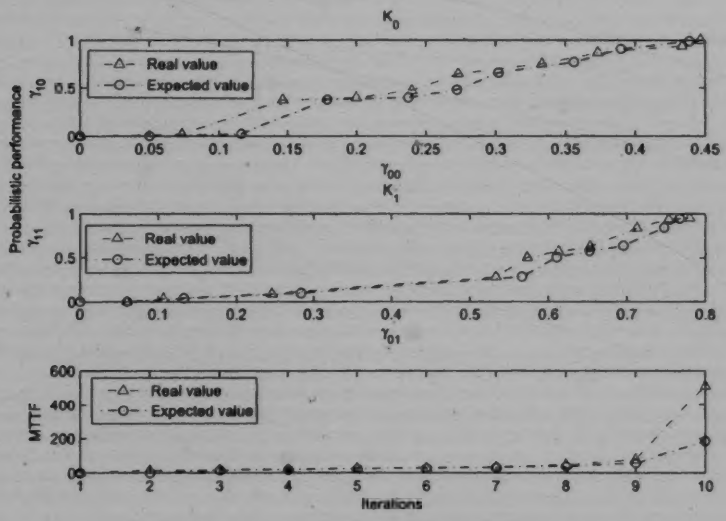

Figure 4.2: Gradient search trajectory.

Figure 4.2 shows a searching trajectory of Algorithms 4.1 and 4.2, where γ_{ij} denotes the probabilistic performance $\Pr\{\|G_{ij}(s,\Delta)\|_\infty \leq \rho_i\}$. In the figure, the first plot shows the related probabilistic performance for controller K_0, the second plot for K_1, and the last one shows the trajectory of MTTF when updating controllers iteratively. In the first two plots, the circles represent the expected performance imposed by the gradient search Algorithm 4.1 in the first design stage, and the triangles represent the achieved probabilistic performance of controllers found by Algorithm 4.2 in the second stage; in the last plot, the circles represent the MTTF based on expected control performance, and the triangles the achieved MTTF using controllers found in Algorithm 4.2. As shown in the figure, the achieved probabilistic performance of controllers increases along the direction of expected performance and is greater than it at each iteration. Moreover, MTTF is strictly increasing iteratively, and the following controllers are obtained that achieve MTTF = 511.5348 minutes:

$$K_0 = \begin{bmatrix} -0.5800 & 0.2251 & -2.1234 & 1.5100 & 4.4991 \\ 3.2406 & 0.5472 & 3.8520 & -0.1351 & -6.5038 \end{bmatrix}, \quad L_0 = \begin{bmatrix} 1.7530 \\ -1.8396 \end{bmatrix},$$

$$K_1 = \begin{bmatrix} -0.5779 & 0.2122 & -2.1297 & 1.5169 & 4.4946 \\ 3.2464 & 0.5368 & 3.8420 & -0.1324 & -6.5095 \end{bmatrix}, \quad L_1 = \begin{bmatrix} 1.7533 \\ -2.0499 \end{bmatrix}.$$

To check the transient performance of the closed-loop system, the side slip responses under regime mode $\zeta(t) = 0$ and $\eta(t) = 0$ for a particular uncertainty sample is shown in Figure 4.3. It is clear that the plant response has similar transient characteristics as the desired one. As the controller is designed for long-term MTTF and probabilistic modeling uncertainties exist in regime models, there may be differences on static gains for a particular uncertainty sample. Overall, the algorithm provides an effective controller design for MTTF.

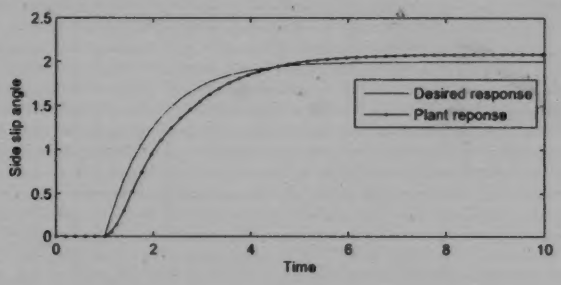

Figure 4.3: Transient responses in a regime model.

4.7 Conclusions

This chapter discusses the design of MTTF suboptimal controller for FTCS's. The reliability criterion is evaluated from a semi-Markov process model which is built based on probabilistic control performance. But, MTTF cannot be written as an analytical expression of controller parameters. Hence, conventional methods are not applicable to controller design with an MTTF objective. To overcome this difficulty, a gradient-based search is first carried out on probabilistic performance parameters; the controller is then updated iteratively to achieve this performance. This two-stage method gives a controller achieving the desired MTTF.

Chapter 5

Semi-Markov FDI model and reliability evaluation*

5.1 Introduction

The Markov models of faults and FDI schemes were initially proposed by Mariton to study the effects of FDI delays on system stability [6]. By using two Markov processes to represent faults and FDI results respectively, Srichander et al. developed the necessary and sufficient conditions for exponential mean-square stability [15]; Mahmoud et al. derived the stability of FTCS's in the presence of noise and summarized their results on the analysis and design of FTCS's based on Markov models [7, 16]. However, Markov models impose a memoryless property [32]. As discussed in [87], the sojourn time duration of FDI is a random variable that may take any probability distribution, but Markov models accept the exponential distribution only. This introduces the so-called memoryless restriction of FDI: the probability of transiting from one state to another is independent of the amount of time that the process has spent in the current state.

This problem was pointed out in [32], but no alternative model was constructed for FDI, and a large quantity of conditional probabilities were used instead. In [87], stability in the presence of general detection delays was analyzed by modeling the sojourn time as a finite state Markov chain or a random variable with a mixture of given probability distributions. But Markov chain model can give only fixed values of sojourn times from a finite set. Also, these distributions can be described by the more general semi-Markov model of FDI proposed in this chapter. Furthermore, the reliability evaluation method presented in Chapter 2 is extended to FTCS's with the semi-Markov FDI description.

*Originally published as: Hongbin Li and Qing Zhao, "Reliability evaluation of fault tolerant control with a semi-Markov fault detection and isolation model", *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering*, vol. 220, no. 5, pp. 329-338, 2006.

Briefly, this chapter is organized as follows: Section 5.2 introduces the model of FTCS's with a semi-Markov FDI description; Section 5.3 presents the reliability evaluation method for FTCS's with this FDI model; an example is given in Section 5.4 to illustrate the semi-Markov FDI model and reliability evaluation procedure; and finally, conclusions are reached in Section 5.5.

5.2 Semi-Markov FDI model

FTCS's are modeled as linear dynamical system with Markov transitions determined by fault and FDI modes. The general form is given by (2.2) in Chapter 2 and also adopted in this chapter but with some modifications to address the limitation of Markov models.

A random variable $\zeta(t) \in S_1 = \{0, 1, 2, \cdots, N_1\}$ called plant mode is adopted to describe fault occurrences among the possible modes in S_1. By assuming that no automatic repair or intermediate fault occurs and that the failure rate is constant, a Markov chain can be used to describe the plant mode [88]. Let $\zeta_n \in S_1$ be a discrete-time Markov chain and define $\zeta(t) = \zeta_n, nT_s \leq t < (n+1)T_s, n \in \mathbb{N}$. $\mathbb{N}$ denotes the set of non-negative integers and T_s the FDI detection cycle duration. The transition probability matrix of ζ_n is denoted as $G = [G_{ij}]_{N_1 \times N_1}, \sum_{j \in S_1} G_{ij} = 1, i \in S_1$.

$\zeta(t)$ is not directly measurable, and the FDI scheme is used to produce an estimate of the plant mode, denoted as $\eta(t) \in S_2 = \{0, 1, \cdots, N_2\}$. Based on $\eta(t)$, the control input $u(\eta(t), t)$ is applied to the plant. In practice, $\eta(t)$ is often generated by cyclic sensor measurements and calculations with a fixed amount of data, e.g., the Shewhart control chart and parity space methods [89]. In this case, the cycle duration time, T_s, can be assumed to be a known constant.

Let $\eta_n \in S_2$ denote a discrete-time stochastic process, $n \in \mathbb{N}$, representing the FDI mode after the n-th detection cycle, as shown in Figure 5.1. Let $\theta_m \in S_2$ and $T_m \in \mathbb{N}$ denote the FDI mode and cycle index respectively after the m-th transition of η_n, $m \in \mathbb{N}$. For example, in Figure 5.1, $\theta_2 = \eta_4$ and $T_2 = 4$.

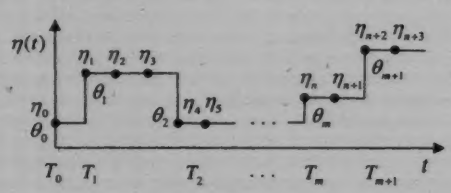

Figure 5.1: A sample path of the FDI process.

$(\theta, T) \triangleq \{\theta_m, T_m : m \in \mathbb{N}\}$ is called a discrete-time Markov renewal process if

$$\begin{aligned} & \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_0, \cdots, \theta_m; T_0, \cdots, T_m\} \\ = \; & \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_m\} \end{aligned} \tag{5.1}$$

holds for fixed $\zeta_{T_m} = \zeta_{T_m+1} = \cdots = \zeta_{T_{m+1}} = k$, $k \in S_1$, $j \in S_2$, $l, m \in \mathbb{N}$. $\eta_n = \theta_m$ is then called the associated discrete-time semi-Markov chain of (θ, T), where $m = \sup_{h \in \mathbb{N}}\{T_h \leq n\}$. The FDI mode at t is defined as $\eta(t) \triangleq \eta_n$, $nT_s \leq t < (n+1)T_s$.

Given $\zeta_{T_m} = \zeta_{T_m+1} = \cdots = \zeta_{T_{m+1}} = k$, $m \in \mathbb{N}$, $k \in S_1$, (θ, T) is called time-homogeneous if

$$Q_\eta^k(i, j, l) \triangleq \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_m = k\}$$

is independent of m for any $i, j \in S_2, l \in \mathbb{N}$. $Q_\eta^k \triangleq \{[Q_\eta^k(i, j, l)]_{N_2 \times N_2}, l \in \mathbb{N}\}$ is called the semi-Markov kernel of η_n given $\zeta_n = k$. Note that the behavior and parameters of η_n depend on ζ_n as η_n is an estimate of ζ_n.

Given $\zeta_n = k$, $k \in S_1$, it can be shown that $\theta \triangleq \{\theta_m : m \in N\}$ is a Markov chain with state space S_2 and transition matrix $P^k \triangleq [P_{ij}^k]_{N_2 \times N_2} \triangleq [\sum_{l=1}^{\infty} Q_\eta^k(i, j, l)]_{N_2 \times N_2}$ [90, 91].

Given $\zeta_{T_m} = \zeta_{T_m+1} \cdots = \zeta_{T_{m+1}} = k$, let $\tau_{ij}^k = T_{m+1} - T_m$ if $\theta_m = i$ and $\theta_{m+1} = j$, $k \in S_1$, $i, j \in S_2$. τ_{ij}^k is the sojourn time of η_n between its transition to state i at T_m and the consecutive transition to j at T_{m+1}. The probability distribution of τ_{ij}^k is given by

$$\Pr\{\tau_{ij}^k = l\} = \Pr\{T_{m+1} - T_m = l | \theta_m = i, \theta_{m+1} = j\} = \frac{Q_\eta^k(i, j, l)}{P_{ij}^k} \tag{5.2}$$

with the convention that $Q_\eta^k(i, j, l)/P_{ij}^k = \mathbf{1}_{\{l=+\infty\}}$ if $P_{ij}^k = Q_\eta^k(i, j, l) = 0$, $i, j \in S_2$, $l \in N$. The indicator function $\mathbf{1}_{\{l=+\infty\}} = 1$ if $l = +\infty$; otherwise, $\mathbf{1}_{\{l=+\infty\}} = 0$. Denote $H^k(i, j, l) \triangleq \Pr\{\tau_{ij}^k = l\}$ and $H^k \triangleq [H^k(i, j, l)]_{N_2 \times N_2}$.

Given $\zeta_n = k$, P^k, together with H^k, determines the stochastic behavior of η_n, or equivalently, Q_η^k solely determines η_n as $Q_\eta^k(i, j, l) = P_{ij}^k H(i, j, l)$.

To recap, the description of FDI is summarized as follows:

1) The FDI mode, η_n, is modeled as a semi-Markov chain conditioning on the plant mode, ζ_n.

2) The embedded Markov renewal process (θ, T) gives the transition history of η_n.

3) Given a fixed plant mode $\zeta_n = k$, P^k describes the transition probability of the embedded Markov chain θ_m and H^k the sojourn time distribution of η_n.

5.3 Reliability modeling

Considering that the plant and FDI modes are described by discrete-time stochastic models and that the fault occurrence within T_s is assumed to be negligible, we are interested in evaluating the reliability value at $t = nT_s$, denoted by $R_n \triangleq R(nT_s)$, $n \in \mathbb{N}$.

The performance measure at $t = nT_s$ is denoted as J_n and the maximum performance threshold when $\zeta_n = i$ is denoted as $J^i_{\max}$, $i \in S_1$. J_n is determined by a performance measure function, such as the system norm of the system model corresponding to ζ_n and η_n. The hard deadline is denoted as $T_{\text{hd}} \in \mathbb{N}$, the maximum number of detection cycles T_s for a temporal performance violation. Based on Definition 2.1, the reliability index R_n is equal to the following probability:

$$R_n = 1 - \Pr\{\exists k \in \mathbb{N}, 0 \leq k < n, n-k > T_{\text{hd}}, \forall l \in \mathbb{N}, k \leq l \leq n, J_l > J^i_{\max}, i = \zeta_l\}.$$

Following similar idea as in Chapter 2, a discrete-time semi-Markov chain X^{R}_n is presented to evaluate this reliability index. For each plant mode i, two functional states of X^{R}_n are defined as follows:

$$i_{\text{N}}: \quad \{\zeta_n = i\} \cap \{J_n \leq J^i_{\max}\}, \tag{5.3}$$

$$i_{\text{F}}: \quad \{\zeta_n = i\} \cap \{J_n > J^i_{\max}\} \cap \{\text{sojourn time} \leq T_{\text{hd}}\}. \tag{5.4}$$

The absorbing semi-Markov state 'F' represents the total failure state of the system. If the initial state $X^{\text{R}}_0 = 0_{\text{N}}$, $R_n = 1 - P^{\text{R}}(0_{\text{N}}, \text{F}, n)$, where $P^{\text{R}}(0_{\text{N}}, \text{F}, n)$ denotes the transition probability from 0_{N} to F at n. Therefore, the reliability evaluation problem is reduced to constructing X^{R}_n and calculating its transition probability.

To calculate the semi-Markov kernel of X^{R}_n, several probabilistic parameters are defined in Chapter 2, which can be naturally extended as shown in the following equations:

$$\gamma_{ij} \triangleq \Pr\{J_n \leq J^i_{\max} | \zeta_n = i, \eta_n = j\}, \ \pi^i_j \triangleq \lim_{n\to\infty} \Pr\{\eta_n = j | \zeta_n = i\},$$
$$w^i_j \triangleq \lim_{n\to\infty} \Pr\{\eta_n = j | X^{\text{R}}_n = i_{\text{N}}\}, \ v^i_j \triangleq \lim_{n\to\infty} \Pr\{\eta_n = j | X^{\text{R}}_n = i_{\text{F}}\},$$

where $i \in S_1$, $j \in S_2$.

Given $\zeta_n = i$ and $\eta_n = j$, the combinational mode (ζ_n, η_n) after the subsequent transition is determined by which one of ζ_n and η_n transits first and which mode they transit to. For example, if ζ_n transits first to k at $n+m$, then $(\zeta_{n+1}, \eta_{n+1}) = \cdots = (\zeta_{n+m-1}, \eta_{n+m-1}) = (i, j)$ and $(\zeta_{n+m}, \eta_{n+m}) = (k, j)$; if η_n transits first to l at $n+m$, then $(\zeta_{n+1}, \eta_{n+1}) = \cdots = (\zeta_{n+m-1}, \eta_{n+m-1}) = (i, j)$ and $(\zeta_{n+m}, \eta_{n+m}) = (i, l)$. So ζ_n

and η_n can be considered to be competing between each other, and the order of transitions is crucial to determine the subsequent mode. We call these transitions competition transitions, and their probabilities competition probabilities, as given in the following definition.

Definition 5.1 *Given $\zeta_n = i$ and $\eta_n = j$, the combinational mode is denoted as (i,j), $i \in S_1, j \in S_2$. Suppose $(\zeta_{n+1}, \eta_{n+1}) = \cdots = (\zeta_{n+m-1}, \eta_{n+m-1}) = (i,j)$ and the next combinational mode after the consequent transition of ζ_n or/and η_n at $n+m$ is $(\zeta_{n+m}, \eta_{n+m}) = (k,l)$, where $k \neq i$ or/and $l \neq j$, $k \in S_1, j \in S_2$. The probability of this event is called the competition probability, denoted by $\rho_{(i,j)\rightarrowtail(k,l)}(m)$.*

Given $\zeta_n = i, \eta_n = j$, the sojourn times of ζ_n and η_n are denoted as σ_i and τ_j^i respectively. If the next mode of η_n is known as l, the sojourn time of η_n is denoted as τ_{jl}^i. If the plant mode i of ζ_n is absorbing, $\Pr\{\sigma_i > \tau_j^i\} = 1$; otherwise,

$$\begin{aligned}
\Pr\{\sigma_i > \tau_j^i\} &= \sum_{m=1}^{\infty} G_{ii}^m \sum_{l \in S_2} P_{jl}^i \sum_{h=1}^{m} H^i(j,l,h), \\
\Pr\{\sigma_i = \tau_j^i\} &= \sum_{m=1}^{\infty} G_{ii}^{m-1}(1-G_{ii}) \sum_{l \in S_2} P_{jl}^i H^i(j,l,m), \\
\Pr\{\sigma_i < \tau_j^i\} &= 1 - \Pr\{\sigma_i > \tau_j^i\} - \Pr\{\sigma_i = \tau_j^i\}.
\end{aligned}$$

The competition probabilities can be classified into following three cases:

$$\begin{aligned}
\rho_{(i,j)\rightarrowtail(i,l)}(m) &= \Pr\{\eta_{n+m} = l \cap \tau_{jl}^i = m | \sigma_i > \tau_j^i\} \Pr\{\sigma_i > \tau_j^i\} \\
&= P_{jl}^i H^i(j,l,m) \Pr\{\sigma_i > \tau_j^i\}, \\
\rho_{(i,j)\rightarrowtail(k,l)}(m) &= \Pr\{\zeta_{n+m} = k \cap \sigma_i = m \cap \eta_{n+m} = l \cap \tau_{jl}^i = m\}. \\
&= G_{ii}^{m-1} G_{ik} P_{jl}^i H^i(j,l,m), \\
\rho_{(i,j)\rightarrowtail(k,j)}(m) &= \Pr\{\zeta_{n+m} = k \cap \sigma_i = m | \sigma_i < \tau_j^i\} \Pr\{\sigma_i < \tau_j^i\} \\
&= G_{ii}^{m-1} G_{ik} \Pr\{\sigma_i < \tau_j^i\},
\end{aligned}$$

where $k \neq i, l \neq j$, and $m \in \mathbb{N}$.

With these probabilistic parameters, the semi-Markov kernel of reliability model X_n^R can be calculated by the following theorem. For notational simplicity, $\rho_{(i,k)\rightarrowtail(j,l)}(m)$ as $\rho_{ik\rightarrowtail jl}$, and $\rho_{(i,k)\rightarrowtail(j,l)}(\min(m, T_{hd}))$ as $\rho_{ik\rightarrowtail jl}^{\min}$.

Theorem 5.1 *The semi-Markov kernel of the reliability semi-Markov chain, X_n^R, is given*

by the following equations:

$$Q_{\mathrm{R}}(i_{\mathrm{N}}, i_{\mathrm{N}}, m) = \sum_{k\in S_2} w_k^i \sum_{l\in S_2} \rho_{ik\rightarrow il}\gamma_{il}, \tag{5.5}$$

$$Q_{\mathrm{R}}(i_{\mathrm{N}}, j_{\mathrm{N}}, m) = \sum_{k\in S_2} w_k^i \sum_{l\in S_2} \rho_{ik\rightarrow jl}\gamma_{jl}, \tag{5.6}$$

$$Q_{\mathrm{R}}(i_{\mathrm{N}}, i_{\mathrm{F}}, m) = \sum_{k\in S_2} w_k^i \sum_{l\in S_2} \rho_{ik\rightarrow il}(1-\gamma_{il}), \tag{5.7}$$

$$Q_{\mathrm{R}}(i_{\mathrm{N}}, j_{\mathrm{F}}, m) = \sum_{k\in S_2} w_k^i \sum_{l\in S_2} \rho_{ik\rightarrow jl}(1-\gamma_{jl}), \tag{5.8}$$

$$Q_{\mathrm{R}}(i_{\mathrm{F}}, i_{\mathrm{N}}, m) = \sum_{k\in S_2} v_k^i \sum_{l\in S_2} \rho^{\min}_{ik\rightarrow il}\gamma_{il}, \tag{5.9}$$

$$Q_{\mathrm{R}}(i_{\mathrm{F}}, j_{\mathrm{N}}, m) = \sum_{k\in S_2} v_k^i \sum_{l\in S_2} \rho^{\min}_{ik\rightarrow jl}\gamma_{jl}, \tag{5.10}$$

$$Q_{\mathrm{R}}(i_{\mathrm{F}}, i_{\mathrm{F}}, m) = \sum_{k\in S_2} v_k^i \sum_{l\in S_2} \rho^{\min}_{ik\rightarrow il}(1-\gamma_{il}), \tag{5.11}$$

$$Q_{\mathrm{R}}(i_{\mathrm{F}}, j_{\mathrm{F}}, m) = \sum_{k\in S_2} v_k^i \sum_{l\in S_2} \rho^{\min}_{ik\rightarrow jl}(1-\gamma_{jl}), \tag{5.12}$$

$$Q_{\mathrm{R}}(i_{\mathrm{F}}, \mathrm{F}, m) = \mathbf{1}_{\{m>T_{\mathrm{hd}}\}}(1 - \sum_{h\in\mathbb{N}, h\le m} \sum_{a\in S_{\mathrm{r}}, a\neq \mathrm{F}} Q_{\mathrm{R}}(i_{\mathrm{F}}, a, h)), \tag{5.13}$$

$$Q_{\mathrm{R}}(\mathrm{F}, a, m) = 0, a \in S_{\mathrm{r}}, \tag{5.14}$$

where T_{hd} denotes the hard deadline, $m \in \mathbb{N}$, $i \in S_1$, $l \neq k$. The indicator function $\mathbf{1}_{\{m>T_{\mathrm{hd}}\}} = 1$ if $m > T_{\mathrm{hd}}$; otherwise, $\mathbf{1}_{\{m>T_{\mathrm{hd}}\}} = 0$.

Proof: $(\phi^{\mathrm{R}}_{n'}, T^{\mathrm{R}}_{n'})$ denotes the associated discrete-time Markov renewal process of X^R_n, $n, n' \in \mathbb{N}$. (θ_h, T_h) denotes the associated Markov renewal process of η_n, $h \in \mathbb{N}$. n, h, and n' represent the cycle or transition indices of these processes, but they may correspond to the same time instant.

The transitions are caused by the changes in the FDI and plant modes. By the total probability formula and conditioning on the FDI modes, the transition probability can be decomposed into three parts, as shown in the following equations:

$$\begin{aligned}
&Q_{\mathrm{R}}(i_{\mathrm{N}}, i_{\mathrm{N}}, m) = \Pr\{\phi^{\mathrm{R}}_{n'+1} = i_{\mathrm{N}}, T^{\mathrm{R}}_{n'+1} - T^{\mathrm{R}}_{n'} = m | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}}\} \\
&= \sum_{k\in S_2} \Pr\{\phi^{\mathrm{R}}_{n'+1} = i_{\mathrm{N}}, T^{\mathrm{R}}_{n'+1} - T^{\mathrm{R}}_{n'} = m | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}} \cap \theta_h = k\} \Pr\{\theta_h = k | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}}\} \\
&= \sum_{k\in S_2} \Pr\{\theta_h = k | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}}\} \sum_{l\in S_2} \Pr\{J_{n+m} \le J^i_{\max} \cap \zeta_{n+1} = \cdots = \zeta_{n+m} = i \cap \\
&\eta_{n+m} = \theta_{h+1} = l \cap T_{h+1} - T_h = m | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}} \cap \theta_h = k)\} \\
&= \sum_{k\in S_2} \Pr\{\theta_h = k | \phi^{\mathrm{R}}_{n'} = i_{\mathrm{N}}\} \sum_{l\in S_2} \Pr\{J_{n+m} \le J^i_{\max} | \zeta_{n+m} = i \cap \eta_{n+m} = l\} \\
&\Pr\{\sigma_i > m \cap \theta_{h+1} = l \cap \tau^i_{kl} = m | \zeta_n = i \cap \theta_h = k\},
\end{aligned} \tag{5.15}$$

where τ_{kl}^i and σ_i denote the sojourn time of ζ_n and η_n respectively. The first two terms in (5.15) can be approximated by the following stationary probabilities in the probabilistic parameters:

$$\Pr\{\theta_h = k | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}}\} \approx w_k^i, \tag{5.16}$$

$$\Pr\{J_{n+m} \leq J_{\max}^i | \zeta_{n+m} = i \cap \eta_{n+m} = l\} \approx \gamma_{il}. \tag{5.17}$$

The last term in (5.15) is equal to the following competition probability:

$$\Pr\{\sigma_i > m \cap \theta_{h+1} = l \cap \tau_{kl}^i = m | \zeta_n = i \cap \theta_h = k\} = \rho_{ik \rightarrow il}. \tag{5.18}$$

Substitute (5.16)-(5.18) to (5.15) and (5.5) is proved. (5.6)-(5.8) can be proved in a similar fashion as shown in the following example of (5.6).

$$\begin{aligned}
& Q_{\mathrm{R}}(i_{\mathrm{N}}, j_{\mathrm{N}}, m) = \Pr\{\phi_{n'+1}^{\mathrm{R}} = j_{\mathrm{N}}, T_{n'+1}^{\mathrm{R}} - T_{n'}^{\mathrm{R}} = m | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}}\} \\
= & \sum_{k \in S_2} \Pr\{\phi_{n'+1}^{\mathrm{R}} = j_{\mathrm{N}}, T_{n'+1}^{\mathrm{R}} - T_{n'}^{\mathrm{R}} = m | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}} \cap \theta_h = k\} \Pr\{\theta_h = k | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}}\} \\
= & \sum_{k \in S_2} \Pr\{\theta_h = k | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}}\} \sum_{l \in S_2} \Pr\{J_{n+m} \leq J_{\max}^i \cap \zeta_{n+1} \cdots = \zeta_{n+m-1} = i \\
& \cap \zeta_{n+m} = j \cap \eta_{n+m} = \theta_{h+1} = l \cap T_{h+1} - T_h = m | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}} \cap \theta_h = k)\} \\
= & \sum_{k \in S_2} \Pr\{\theta_h = k | \phi_{n'}^{\mathrm{R}} = i_{\mathrm{N}}\} \sum_{l \in S_2} \Pr\{J_{n+m} \leq J_{\max}^i | \zeta_{n+m} = j \cap \eta_{n+m} = l\} \\
& \Pr\{\zeta_{n+m} = j \cap \sigma_i = m \cap \eta_{n+m} = l \cap \tau_{kl}^i = m | \zeta_n = i \cap \theta_h = k\} \\
= & \sum_{k \in S_2} w_k^i \sum_{l \in S_2} \rho_{ik \rightarrow jl} \gamma_{jl},
\end{aligned} \tag{5.19}$$

where $j \neq i$, $j \in S_1$.

For (5.10)-(5.13), when the sojourn time is no greater than T_{hd}, the transition is similar to the case of i_{N}; otherwise, X_n^{R} transits to F. Therefore, the minimum function $\min(m, T_{\mathrm{hd}})$ is used in (5.10)-(5.12); $Q_{\mathrm{R}}(i_{\mathrm{F}}, \mathrm{F}, m)$ becomes nonzero only if $m > T_{\mathrm{hd}}$, and this probability is complementary to the transition probability to other states within T_{hd}, which is calculated based on $1_{\{m > T_{\mathrm{hd}}\}}$ in (5.13). ■

Remark 5.1 *The main idea of the above derivation of the transition probability is to decompose it into three parts: the FDI mode estimation, the competition probability and the probabilistic performance estimation. The effects of the hard deadline are described by* $\min(m, T_{\mathrm{hd}})$ *and* $1_{\{m > T_{\mathrm{hd}}\}}$.

Once the semi-Markov kernel of X_n^{R} is obtained, the transition probability and reliability function R_n can be calculated using available formulas [90, 91].

5.4 Example

Consider a longitudinal vertical takeoff and landing aircraft model in the form of (2.2) with the following system matrices [92]. The subscript '0' and '1' in the system matrices represent those for plant mode '0' and '1' respectively. Plant mode '0' represents the fault-free mode. Under plant mode '1', an actuator fault is considered, and the effectiveness of the first actuator is reduced by half, as reflected in B_1.

$$A_0 = \begin{bmatrix} -0.0366 & 0.0271 & 0.0188 & -0.4555 \\ 0.0482 & -1.01 & 0.0024 & -4.0208 \\ 0.1002 & 0.3681 & -0.707 & 1.420 \\ 0 & 0 & 1.0 & 0 \end{bmatrix}, \; B_0 = \begin{bmatrix} 0.4422 & 0.1761 \\ 3.5446 & -7.5922 \\ -5.52 & 4.49 \\ 0 & 0 \end{bmatrix},$$

$$B_1 = \begin{bmatrix} 0.2211 & 0.1761 \\ 1.7723 & -7.5922 \\ -2.76 & 4.49 \\ 0 & 0 \end{bmatrix}, \; C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \; A_1 = A_0, \; C_1 = C_0,$$

$$E_0 = [0.05 \;\; 0.05 \;\; 0.05 \;\; 0.05]^T, \; E_1 = E_0.$$

Suppose the cycle duration, T_s, is 1 second. The transition matrix of the plant mode Markov chain ζ_n is

$$G = \begin{bmatrix} 0.99 & 0.01 \\ 0 & 1 \end{bmatrix}.$$

According to G, the mean time for the fault occurrence is 1/0.01 = 100 cycles = 100 seconds, and this high failure rate is intentionally chosen for this example to reduce the calculation burden. The FDI is modeled by a semi-Markov chain η_n with the following parameters:

$$P^0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; P^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$H^0(0,1,m) = H^1(1,0,m) = \text{Pois}(m|20),$$

$$H^0(1,0,m) = H^1(0,1,m) = \text{Bin}(m|10,0.5),$$

where P^0 and P^1 are transition probability matrices of the embedded Markov chain and $H^0(0,1,m)$, $H^0(1,0,m)$, $H^1(0,1,m)$, $H^1(1,0,m)$ are distribution functions of sojourn time, $m \in \mathbb{N}$. 'Pois$(\cdot|\cdot)$' and 'Bin$(\cdot|\cdot,\cdot)$' denote the Poisson and Binomial distributions respectively:

$$\text{Pois}(m|20) = \frac{20^m}{m!}e^{-20},$$

$$\text{Bin}(m|10,0.5) = \frac{10!}{m!(10-m)!}0.5^m 0.5^{10-m}, m \leq 10.$$

Based on these parameters, the stationary distribution of η_n is computed as

$$\begin{bmatrix} \pi_0^0 & \pi_1^0 \\ \pi_0^1 & \pi_1^1 \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{bmatrix},$$

which shows that the correct and false detection probabilities are 0.8 and 0.2 respectively.

The differences between Markov and semi-Markov model of FDI can be shown in the sample paths from these two types of models given in Figure 5.2. These two curves are given under the plant mode '0', and the generator matrix of the continuous-time Markov process model is

$$G' = \begin{bmatrix} -0.05 & 0.05 \\ 0.2 & -0.2 \end{bmatrix}.$$

According to G', the stationary distribution is [0.8 0.2], the same as $[\pi_0^0\ \pi_1^0]$. Furthermore, the mean sojourn times from mode 0 to 1 and from 1 to 0 are 20 and 5 seconds respectively, the same as the means of $H^0(0,1,m)$ and $H^1(1,0,m)$. However, in the sample path of the Markov process model in Figure 5.2, there are 2 transitions from 1 to 0 with a sojourn time of about 0.05 of a second due to the memoryless property of exponential distribution. These transitions are impractical because the FDI needs at least one detection cycle to return mode 0 from the false alarm. In contrast, the sample path from the semi-Markov model is acceptable: each sojourn time is an integer multiple of the detection cycle duration. Therefore the Markov model may not generate a reasonable sample path for FDI with cyclic detection schemes.

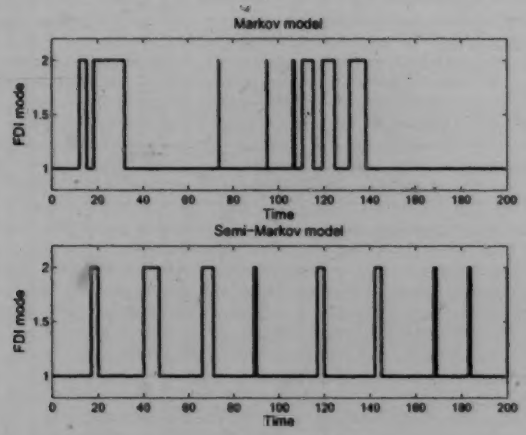

Figure 5.2: Sample paths of FDI models.

The static state feedback controller for the normal and faulty cases are:

$$K_0 = \begin{bmatrix} -0.4558 & -0.5080 & 1.4881 & 1.0242 \\ -0.1022 & 0.1089 & 0.1216 & 0.0486 \end{bmatrix},$$

$$K_1 = \begin{bmatrix} -0.1078 & 0.7452 & 0.3158 & 0.6761 \\ 0.1680 & 1.3673 & -0.7858 & -0.4397 \end{bmatrix}.$$

When $\eta(t) = 0$, $u = K_0 x$ is in use; when $\eta(t) = 1$, $u = K_1 x$ is switched on.

Here, we use the $\mathcal{H}_\infty$ norm as the performance measure. The performance evaluation function with the thresholds for the two fault modes is defined as follows:

$$J_n \doteq \begin{cases} 1, \text{ unstable at } n, \\ \frac{\|G_{yw}(\zeta_n, \eta_n, s)\|_\infty}{1+\|G_{yw}(\zeta_n, \eta_n, s)\|_\infty}, \text{ stable at } n, \end{cases}$$

$$J^0_{\max} = 0.5, \quad J^1_{\max} = 0.67,$$

where $G_{yw}(\zeta_n, \eta_n, s)$ is the transfer function from w to y corresponding to the current fault mode ζ_n and the FDI mode η_n. According to the assumption of known probability distributions of modeling uncertainties and the randomized algorithm in [46], the following probabilistic performance values can be obtained:

$$\begin{bmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \end{bmatrix} = \begin{bmatrix} 0.7033 & 0.6260 \\ 0.5583 & 0.6084 \end{bmatrix}.$$

For example, γ_{00} means $\Pr\{J_n \le J^0_{\max} | \zeta_n = 0 \cap \eta_n = 0\} = 0.7033$.

Other probabilistic parameters are calculated as follows:

$$\begin{bmatrix} w_{00} & w_{01} \\ w_{10} & w_{11} \end{bmatrix} = \begin{bmatrix} 0.6920 & 0.3080 \\ 0.3145 & 0.6855 \end{bmatrix}, \quad \begin{bmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{bmatrix} = \begin{bmatrix} 0.6134 & 0.3866 \\ 0.3606 & 0.6394 \end{bmatrix}.$$

For example, $\Pr\{\eta_n = 0 | X^{\mathrm{R}}_n = 0^{\mathrm{N}}\} \approx w_{00} = 0.6920$.

Set the hard deadline $T_{\mathrm{hd}} = 5$. By substituting these parameters into Theorem 5.1, we obtain the semi-Markov reliability model. The transition probability and reliability function curve are then calculated, as shown in Figure 5.3, where R_n is the reliability curve and $P^{\mathrm{R}}(1, i, n)$ the transition probability curve from state #1, 0_{N}, to state $\#i$, $i = 1 \sim 5$, $n \in \mathbb{N}$. From $P^{\mathrm{R}}(1, 1, n)$ and $P^{\mathrm{R}}(1, 2, n)$, we can see that the performance degradation during this time period is mainly caused by false alarms of FDI and X^{R}_n jumps from 0_{N} to 0_{F} with high probability. From R_n and $\mathbf{P}^{\mathrm{R}}(1, 5, n)$, we can see that the probability of system failure is zero within T_{hd}, a finding which is consistent with our definition of reliability function.

Next, in order to show the influence of FDI on reliability, we use the same aircraft model but with a different FDI, which has the following new parameters:

$$H^0(0, 1, m) = H^1(1, 0, m) = \mathrm{Pois}(m|80),$$

$$H^0(1, 0, m) = H^1(0, 1, m) = \mathrm{Bin}(m|3, 0.5).$$

According to $H^0(0, 1, m)$, the mean sojourn time for a false alarm increases from 20 to 80 T_{s}; according to $H^0(1, 0, m)$, the mean recovery time from a false alarm decreases from 10

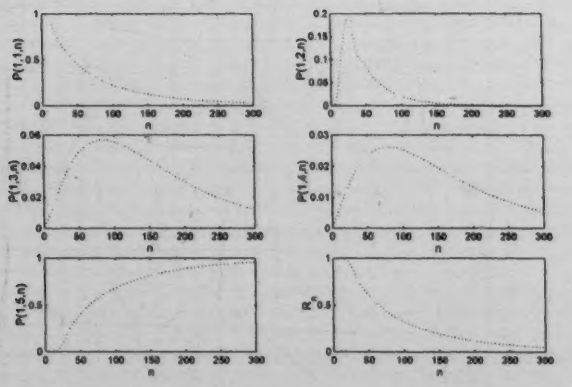

Figure 5.3: Transition probability and reliability curves.

to 3 T_s. Following the same procedure, the transition probability curves of the reliability model and the reliability curve are given in Figure 5.4. Compared with the results in Figure 5.3, the maximum transition probability to state #2 decreases approximately from 0.2 to 0.08, and the maximum point shifts from $n = 20$ to $n = 80$ as a result of the increase in the mean time for false alarms. We also note that the shapes of some of the curves are very different from those in Figure 5.3. Consequently, the transition probability to state #5 decreases and the reliability deteriorates more slowly and the system will probably survive longer. Therefore, a properly designed FDI is crucial to achieve high reliability of FTCS's.

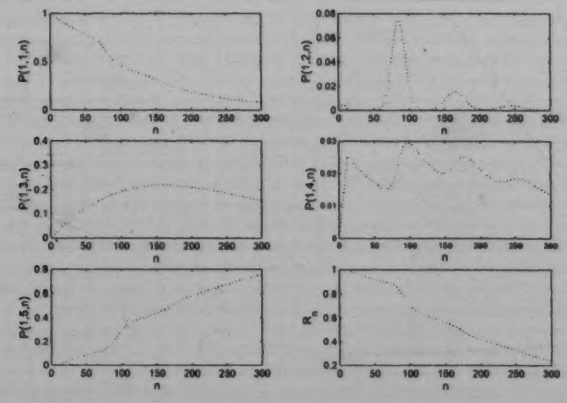

Figure 5.4: Transition probability and reliability curves with a different FDI.

5.5 Conclusions

This chapter presents a semi-Markov description of FDI and the reliability evaluation of FTCS's with a semi-Markov FDI model. This semi-Markov model of FDI is more general than the Markov process model, and the memoryless restriction is thereby removed. The reliability evaluation method presented in Chapter 2 is then extended to this general FTCS's model. This reliability evaluation considers the characteristics of FTCS's, and an example is given to illustrate the procedure.

Chapter 6

Reliability monitoring*

6.1 Introduction

In previous chapters, we considered static model-based control objectives and built a semi-Markov model based on imperfect FDI and hard-deadline concepts. However, in many practical systems, the safety and reliability of operation are often assessed based on dynamic system responses. For instance, reliability in structural control is defined as the probability of system outputs outcrossing safety boundaries and evaluated by using Gaussian approximation [93]. Also, an online available reliability monitoring scheme using updated information may aid maintenance scheduling, provide pre-alarming, and avoid emergent overhauls. How to evaluate reliability when it is defined on system trajectory and how to implement an online-monitoring scheme are the main motivations of this chapter.

The objectives of this chapter are three-fold. First of all, a Steady State Test (SST) is proposed to reduce false alarms of FDI decisions. The stochastic modeling of such an FDI scheme is studied based on which the transition characteristics of FDI modes can be described. The second objective is to develop a reliability evaluation scheme for FTCS's based on system dynamic responses and safety boundary. At last, online monitoring features are considered, such as estimation of FDI transition parameters based on history data and timely update of reliability index to reflect up-to-date system behavior.

The remainder of this chapter is organized as follows: The assumptions and system structure are given in Section 6.2; FDI scheme, modeling, and parameter estimation are discussed in Section 6.3; the determination of out-crossing failure rates and hard-deadlines are discussed in Section 6.4; and the reliability model construction is discussed in Section 6.5 followed by a demonstration example of an F-14 aircraft model in Section 6.6.

*Results presented in this chapter has been submitted to a special issue in the *Journal of Control Science and Engineering*.

6.2 Assumptions and system structure

Assumption 6.1 *The considered plant is assumed to have finite fault modes, and dynamics under each fault mode can be effectively represented by a linear system model.*

Fault modes are represented by a set S with N integers; $\{\mathcal{M}_i : i \in S\}$ represents the set of dynamical plant models under various fault modes; and $\{\mathcal{K}_j : j \in S\}$ denotes a set of reconfigurable controllers in a switching structure. $\mathcal{K}_j$ is designed for fault mode j based on $\mathcal{M}_j$, $j \in S$. However, true fault modes are usually not directly known, so an FDI scheme is used to generate estimates of fault modes, which may deviate from true fault modes with error probabilities.

Assumption 6.2 *FDI scheme is assumed to generate a fault estimate based on a batch of measurements and calculations for every fixed period T_s.*

This assumption states a cyclic feature of FDI, such as statistical tests and Interactive Multiple Model (IMM) Kalman filters [94]. Discussions in this paper are not restricted to specific design schemes. FDI modes are represented by a discrete-time stochastic process $\eta_n \in S$, where $n \in \mathbb{N}$, the set of non-negative integers. The time duration between consecutive discrete indices is equal to FDI detection period T_s. $\mathcal{K}_j$ is put in use when $\eta_n = j$, $j \in S$. Corresponding to η_n, a discrete-time stochastic process ζ_n denotes true fault mode. In reliability engineering, constant failure rates are usually assumed for the main part of component life cycle. In such a case, ζ_n can be described as a Markov chain [88], and its transition probabilities are denoted as $G_{ij} = \Pr\{\zeta_{n+1} = j | \zeta_n = i\}$, $i, j \in S$.

Assumption 6.3 *System performance is assumed to be represented by a vector signal $z(t)$. Safety region, denoted as Ω, is assumed to a fixed region in space of $z(t)$ bounded by its safety threshold. Failure is assumed to occur when $z(t)$ exists a safety region for the first time.*

This assumption intends to define an appropriate reliability index based on system dynamical response. It is common in control systems to use a signal $z(t)$ to represent performance; and $z(t)$ is usually to be kept at small values against excitations from exogenous disturbances, model uncertainties, and model characteristic changes caused by faults. Safety region Ω is assumed to be fixed and known a priori. The scenario that $z(t)$ exists Ω represents lost of control and system failures. More discussions on this assumption can be found in [75].

Definition 6.1 *For a time interval from 0 to t, the reliability function $R(t)$ is defined as the*

following probability:

$$R(t) = \Pr\{\forall 0 \le \tau \le t,\ z(\tau) \in \Omega\}.$$

Compared with ζ_n and η_n, $z(t)$ is typically a fast-changing function determined by both continuous and discrete dynamics. ζ_n and η_n are two regime modes and determine the transitions among regime models. When $\zeta_n = i$ and $\eta_n = j$ are fixed, $z(t)$ evolves according to plant model $\mathcal{M}_i$ and controller $\mathcal{K}_j$. As a result of this hybrid dynamics, directly evaluating $R(t)$ and MTTF is a difficult problem. Therefore, a discrete-time semi-Markov chain X_n^{R} is constructed for reliability evaluation purpose as in previous chapters. The main idea is: the hybrid system is decomposed into various regime models; each regime model is then evaluated for related safety characteristics; and X_n^{R} is constructed to integrate these characteristics with transition parameters of regime modes and to solve its transition probabilities for reliability evaluation. The structure and main components of reliability monitoring scheme are illustrated in Figure 6.1.

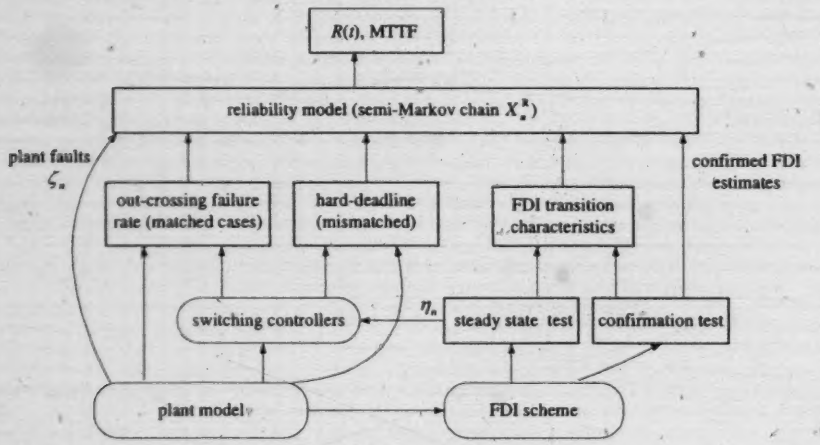

Figure 6.1: System structure.

Semi-Markov reliability model X_n^{R} is the kernel component for calculating MTTF. It is constructed based on the following parameters: 1) the transition rates of ζ_n, called plant failure rates; 2) the estimates of ζ_n from FDI and confirmation test, called confirmed fault modes; 3) the parameters of η_n estimated from history data, called FDI transition characteristics; 4) the probability of $z(t)$ crossing safety boundary during an FDI cycle T_s when $\zeta_n = \eta_n$, called failure out-crossing rates. 5) the average number of periods before crossing safety boundary when $\zeta_n \neq \eta_n$, called hard-deadlines. Among these parameters, the second and third ones can be updated online.

6.3 FDI scheme and its characterization

6.3.1 Steady state tests

It is well-known that false alarm and missing detection rates are two conflicting quality criteria of FDI. One is usually improved at the cost of degrading the other. What is worse, the general rules of adjusting FDI to improve these two criteria simultaneously are often not known. For example, in a scheme based on IMM Kalman filters, it is not clear how to determine Markov interaction parameters. Considering that most false alarms last for short time only, an SST strategy is adopted for post-processing FDI decisions.

SST requires that, when FDI decision changes, new decision is accepted only when it stays the same for a minimum number of detection cycles. Let $T_{SST,j}$ denote the required number of consistent cycles for FDI mode j, $j \in S$. The effectiveness of this SST strategy relies on the distribution of false alarm durations. For example, if a nonnegative discrete random variable λ_0 denotes the false alarm duration when system fault mode $\zeta_n = 0$, T_{SST0} can be taken as $(1-\alpha)$-quantile of λ_0, $0 < \alpha < 1$, meaning

$$\Pr\{\lambda_0 > T_{SST0}\} \leq \alpha,$$

which implies that false alarm probability can be reduce by ratio α when accepting FDI decisions after T_{SST0}. The weakness of this method is additional detection time delay of $T_{SST,j}$ when fault occurs. However, this happens only under rare occurrences of faults. Compared with the improvement on relatively more frequently transitions of FDI modes, this weakness is acceptable.

Detection decisions from SST are represented by η_n and used for controller reconfigurations. In Figure 6.1, the confirmation test is an SST with large test period to further reduce false alarms to a negligible level. It generates confirmed fault modes, which are used with FDI trajectories for updating transition parameters of η_n and reliability index.

6.3.2 Stochastic models

Following methods in Chapter 5, η_n is modeled as a discrete sem-Markov process. Its sample path when applying SST is given in Figure 6.2. Let $\theta_m \in S$ and $T_m \in \mathbb{N}$ denote the FDI mode and cycle index respectively after the m-th transition of η_n, $m \in \mathbb{N}$. For example, in Figure 5.1, $\theta_1 = \eta_5$ and $T_2 = 5$. θ_m and T_m together determine FDI trajectory, and $\eta_n = \theta_{S_n}$, where $S_n = \sup\{m \in \mathbb{N} : T_m \leq n\}$ is the discrete-time counting process of the number of jumps in $[1, n]$. $(\theta, T) \triangleq \{\theta_m, T_m : m \in \mathbb{N}\}$ is called a discrete-time

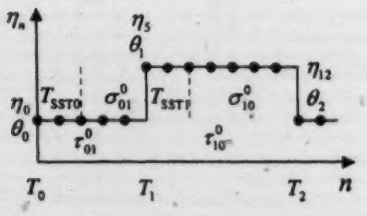

Figure 6.2: A sample path of η_n.

Markov renewal process if

$$\begin{aligned} & \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_0, \cdots, \theta_m; T_0, \cdots, T_m\} \\ = \; & \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_m\} \end{aligned}$$

holds for fixed $\zeta_{T_m} = \zeta_{T_m+1} = \cdots = \zeta_{T_{m+1}} = k$, where $k \in S_1$, $j \in S_2$, and $l, m \in \mathbf{N}$. $\eta_n = \theta_m$ is then called the associated discrete-time semi-Markov chain of (θ, T). It can be shown that θ_m is a Markov chain, and its transition probability matrix is denoted by P^k.

Given $\zeta_{T_m} = \zeta_{T_m+1} \cdots = \zeta_{T_{m+1}} = k$, let $\tau^k_{ij} = T_{m+1} - T_m$ if $\theta_m = i$ and $\theta_{m+1} = j$, where $i, j \in S_2$ and $k \in S_1$. τ^k_{ij} is the sojourn time of η_n between its transition to state i at T_m and the consecutive transition to j at T_{m+1}. If the transition destination state is not specified, let τ^k_i denote the sojourn time at state i.

As shown in Figure 6.2, τ^k_{ij} is the sum of two variables: a constant $T_{\text{SST}i}$ for SST period and a random sojourn time σ^k_{ij}. Let $h^k_{ij}(l)$ and $g^k_{ij}(l)$ denote the discrete distribution functions of τ^k_{ij} and σ^k_{ij} respectively, which have the following relations:

$$h^k_{ij}(l) = \Pr\{\tau^k_{ij} = l\} = \begin{cases} 0, & l \le T_{\text{SST}i}; \\ g^k_{ij}(l - T_{\text{SST}i}), & l \le T_{\text{SST}i}. \end{cases} \tag{6.1}$$

Semi-Markov description provides a general model on FDI mode transitions, but it involves a large number of parameters. The transition characteristics of η_n are jointly determined by P^k and h^k_{ij} (or g^k_{ij}). If S contains N fault modes, there are N transition probability matrices P^k and N^3 distribution functions h^k_{ij}. If each h^k_i follows geometric distribution, the description of η_n may degenerate to a hypothetical Markov model η'_n.

Markov chain can be considered as a special type of semi-Markov chain. If η_n can be modeled as a Markov chain with transition probability matrix denoted by H^k for $\zeta_n = k$,

the following relations hold:

$$P_{ij}^k = \frac{H_{ij}^k}{1 - H_{ii}^k}, \tag{6.2}$$

$$h_{ij}^k(l) = (H_{ii}^k)^{l-1} H_{ij}^k, \tag{6.3}$$

$$h_i^k(l) = (H_{ii}^k)^{l-1}(1 - H_{ii}^k), \tag{6.4}$$

It is obvious that h_i^k is a geometric distribution. In fact, this is an essential property of Markov chain: A discrete-time semi-Markov chain degenerates to a Markov chain if and only if the sojourn time at each state (when subsequent state is not specified) follows geometric distribution.

When T_{SST} is nonzero, the sojourn time of η_n does not follow geometric distribution owing to this deterministic constant. However, as T_{SST} is known, a hypothetical process η'_n can be constructed by setting T_{SST} to zeros; if the sojourn time of η'_n is geometrically distributed, it can be described as a Markov chain; the original sojourn time of η_n can be recovered by adding T_{SST} to that of η'_n. This method may greatly reduce the number of parameters for characterizing FDI results.

6.3.3 Transition parameter estimation

FDI transition parameters can be estimated as an off-line test on FDI when both fault mode and FDI detection results are known. This estimation can also be carried out online using FDI history data and confirmed fault modes.

When η_n is modeled as a semi-Markov chain, P^k and h_{ij}^k (or g_{ij}^k) are parameters to be estimated. P^k can be estimated from the transition history of η_n. For example, when ζ_n is kept as a constant k, if there are M_{ij} transitions from i to j among all M transitions leaving i, the ij-th element of P^k can be estimated as $\hat{P}_{ij}^k = M_{ij}/M$.

The estimation of sojourn time distribution g_{ij}^k can be completed in two steps: the histogram of sojourn time is firstly examined to select a standard distribution such that nonparametric estimation is converted to a parametric one; $\hat{g}_{ij}^k$ is then obtained by estimating unknown parameters in distribution functions.

If $\hat{g}_{ij}^k$ follows geometric distribution for all $i, j, k \in S$, η_n can be described as a hypothetical Markov chain η'_n under the hypothesis that $T_{\mathrm{SST}i} = 0$. As a result, transition probability H_{ij}^k from i to j and sojourn time τ_i^k at i have following relation:

$$\Pr\{\tau_i^k = n\} = (H_{ii}^k)^{n-1}(1 - H_{ii}^k).$$

Therefore, $E(\tau_i^k) = \frac{1}{1-H_{ii}^k}$, and H_{ii}^k can be estimated by

$$\hat{H}_{ii}^k = \begin{cases} 1 - \frac{1}{\sum_{l=1}^{M} \tau_i^k(l)/M}, & \sum_{l=1}^{M} \tau_i^k(l)/M \neq 0, \\ 1, & \text{otherwise}, \end{cases} \tag{6.5}$$

where $\tau_i^k(l)$ denote M sojourn time samples at state i, $l = 1, \cdots, M$. H_{ij}^k can be estimated based on the transition frequency from state i to j:

$$\hat{H}_{ij}^k = (1 - \hat{H}_{ii}^k) w_{ij}^k / M, \tag{6.6}$$

where $1 - \hat{H}_{ii}^k$ is a normalization coefficient and w_{ij}^k represents the number of FDI transitions from i to j.

6.4 Out-crossing failure rates and hard-deadlines

Owing to FDI delays or incorrect decisions, controller $\mathcal{K}_i$ may be used for its designated regime model $\mathcal{M}_i$ (namely, matched cases) and other model $\mathcal{M}_j$, $i \neq j$ (namely, mismatched cases). Matched cases usually account for major operation time, while mismatched cases often appear as temporary operation.

Definition 6.2 *The out-crossing failure rate in matched cases is defined as*

$$v_{ii} \triangleq \Pr\{\exists \tau,\ nT_s < \tau \leq (n+1)T_s,\ z(\tau) \notin \Omega | z(nT_s) \in \Omega,\ \zeta_n = \eta_n = i\},\ i \in S$$

Monte Carlo simulation can be used for estimating v_{ii}: At each sample simulation, system is run based on generated sample uncertain plant model and sample disturbance input, and the simulation time when system fails is called a sample time-to-failure. With a large number of time-to-failure samples obtained, v_{ii} can be estimated as the ratio between T_s and sample mean of time-to-failure.

Mismatched cases are usually temporary operation caused by FDI false alarms or delays, and system may return to matched cases if $z(t)$ does not diverge to unsafe region. So, it is important to find out the average tolerable time before system failure. This time limit is called hard-deadline, denoted by $T_{\text{hd}ij}$ for $\zeta_n = i$ and $\eta_n = j$. It can also be estimated by sample mean of time-to-failure using Monte Carlo simulations.

6.5 Reliability model construction

The states of semi-Markov chain X_n^{R} are classified into two groups: one unique failure state, denoted by s_{F}, and multiple functional states, defined as state combinations of $\zeta_n = i$

and $\eta_n = j$, denoted as s_{ij}, where $i \in S_1$ and $j \in S_2$. For example, if two types of faults are considered in the plant, and ζ_n includes states of fault-free, fault type 1, fault type 2, and both fault 1 and 2, represented by $S = \{0, 1, 2, 3\}$; and FDI mode η_n also takes value in S. X_n^{R} then has $4 \times 4 + 1 = 17$ states.

The semi-Markov kernel of X_n^{R} is denoted as $Q(\cdot, \cdot, n)$, representing the one-time transition probability in n steps. It is determined by the following parameters: 1) transition characteristics of fault and FDI modes; 2) outcrossing failure rate in state s_{ii} denoted by v_{ii}; 3) hard-deadline in state s_{ij} denoted by $T_{\mathrm{hd}ij}$; 4) FDI SST period denoted by $T_{\mathrm{SST}j}$ for FDI mode j.

Let us begin with the case that FDI mode can be described as a hypothetical Markov chain η_n' with transition probability denoted by H_{ij}^k. The calculation of Q is classified into the following cases:

Case 1: The transitions from functional states to themselves are not defined and the corresponding elements are assigned as zeros:

$$Q(s_{ii}, s_{ii}, m) = 0, \;\; Q(s_{ij}, s_{ij}, m) = 0, i \in S_1, j \in S_2$$

Case 2: Failure state s_{F} is absorbing:

$$Q(s_{\mathrm{F}}, s_{\mathrm{F}}, m) = \begin{cases} 1, & m = 1; \\ 0, & m > 1. \end{cases}$$

Case 3: Matched states s_{ii}:

$$\begin{aligned}
Q(s_{ii}, s_{\mathrm{F}}, m) &= \begin{cases} (1 - v_{ii})^{m-1} G_{ii}^{m-1} v_{ii}, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i} - 1)} v_{ii}, & m > T_{\mathrm{SST}i}, \end{cases} \\
Q(s_{ii}, s_{ji}, m) &= \begin{cases} (1 - v_{ii})^{m-1} G_{ii}^{m-1} (1 - v_{ii}) G_{ij}, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i} - 1)} (1 - v_{ii}) G_{ij} H_{ii}^i, & m > T_{\mathrm{SST}i}, \end{cases} \\
Q(s_{ii}, s_{ij}, m) &= \begin{cases} 0, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i} - 1)} (1 - v_{ii}) G_{ii} H_{ij}^i, & m > T_{\mathrm{SST}i}, \end{cases} \\
Q(s_{ii}, s_{kj}, m) &= \begin{cases} 0, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{jj}^k]^{(m - T_{\mathrm{SST}i} - 1)} (1 - v_{ii}) G_{ik} H_{ij}^i, & m > T_{\mathrm{SST}i}, \end{cases}
\end{aligned}$$

where $p_{ii} = \Pr\{X_1 = X_2 = \cdots = X_{T_{\mathrm{SST}i}} = s_{ii} | X_0 = s_{ii}\} = (1 - v_{ii})^{T_{\mathrm{SST}i}} G_{ii}^{T_{\mathrm{SST}i}}$, $i \neq j$, $k \neq i, i, j, k \in S$.

The derivation of these equations are based on Markov transition probabilities and the decomposition of each event. For example,

$$\begin{aligned}
Q(s_{ii}, s_{\mathrm{F}}, m) &= \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii}, X_m = s_{\mathrm{F}} | X_0 = s_{ii}\} \\
&= \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} \Pr\{X_1 = s_{\mathrm{F}} | X_0 = s_{ii}\}.
\end{aligned}$$

Considering steady state test of FDI, if $m \leq T_{\text{SST}i}$,

$$\Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} = (1 - v_{ii})^{m-1} G_{ii}^{m-1};$$

If $m > T_{\text{SST}i}$,

$$\begin{aligned} & \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} \\ = \; & \Pr\{X_1 = X_2 = \cdots = X_{T_{\text{SST}i}} = s_{ii} | X_0 = s_{ii}\} [(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\text{SST}i} - 1)}. \end{aligned}$$

Combing these two probabilities with $\Pr\{X_1 = s_{\text{F}} | X_0 = s_{ii}\} = v_{ii}$, $Q(s_{ii}, s_{\text{F}}, m)$ is obtained.

Case 4: Mismatched states: s_{ij}, $i \neq j$. When $m \leq T_{\text{SST}j}$, the transition probability of X_n^{R} to any other state is zero because of SST period. When $T_{\text{SST}j} < m \leq T_{\text{hd}ij}$, the probability of X_n^{R} transiting to any other state is zero except to s_{ii}. The above reasoning is based on the facts that FDI rarely jumps to other false modes when current mode is incorrect, and mean fault occurrence time is in a much higher order compared with a short false FDI detection period. Therefore, when $T_{\text{SST}j} < m \leq T_{\text{hd}ij}$,

$$\begin{aligned} Q(s_{ij}, s_{\text{F}}, m) &= 0, \\ Q(s_{ij}, s_{ii}, m) &= [H_{jj}^i]^{m - T_{\text{SST}j} - 1} H_{ji}^i, \;\; j \neq l, \;\; j, l \in S. \end{aligned}$$

When $m > T_{\text{hd}ij} + 1$, X_n^{R} jumps to s_{F} at the earliest time $m = T_{\text{hd}ij} + 1$ only:

$$\begin{aligned} Q(s_{ij}, s_{\text{F}}, T_{\text{SST}i} + 1) &= 1 - \sum_{k = T_{\text{SST}i} + 1}^{T_{\text{hd}ij}} Q(s_{ij}, s_{ii}, m) \\ &= 1 - \frac{1 - (H_{jj}^i)^{T_{ij} - T_{\text{SST}j} + 1}}{1 - H_{jj}^i} H_{ji}^i. \end{aligned}$$

In the general cases, η_n is modeled as a semi-Markov chain, and the competition probabilities methods discussed in Chapter 5 can be utilized. As the states of X_n^{R} is mainly defined as the state combinations of ζ_n and η_n, the calculation of the semi-Markov kernel of X_n^{R} is simplified when competition probability $\rho_{(i,j) \rightarrowtail (k,l)}(m)$ is available, as shown in

the following formulas:

$$
\begin{aligned}
Q(s_{ii}, s_{kl}, m) &= (1 - v_{ii})^m \rho_{(i,i)\rightarrow(k,l)}(m), \\
Q(s_{ii}, s_F, m) &= (1 - v_{ii})^{m-1} v_{ii}, \\
Q(s_{ii}, s_{ii}, m) &= 0, \\
Q(s_{ij}, s_{kl}, m) &= \begin{cases} \rho_{(i,j)\rightarrow(k,l)}(m), & m \leq T_{\text{hd}ij} \text{ and } k = l = i, \\ 0, & \text{otherwise} \end{cases} \\
Q(s_{ij}, s_F, m) &= \begin{cases} 0, & m \leq T_{\text{hd}ij}, \\ 1 - \sum_{m=1}^{T_{\text{hd}ij}} Q(s_{ij}, s_{ii}, m), & m > T_{\text{hd}ij}, \end{cases} \\
Q(s_F, s_F, m) &= \begin{cases} 1, & m = 1; \\ 0, & m > 1. \end{cases}
\end{aligned}
$$

Although these formulas appear to be simpler, both the parameter estimation and competition probability calculations need much more calculation burden than the first case when FDI decision is modeled as a hypothetical Markov chain. Once X_n^{R} is constructed, calculation of reliability function and MTTF are straightforward using available formulas [27].

6.6 Example

6.6.1 Model description

The F-14 aircraft control example used in Chapter 2 is used again to demonstrate the reliability monitoring scheme [47]. The description and system diagram can be found in Chapter 2 and are omitted here for brevity.

The control objectives are to have handling quality (HQ) responses from lateral stick to roll rate p and from rudder pedal to side-slip angle β match ideal HQ models. Under fault free modes, the HQ models are $5\frac{2}{s+2}$ and $-2.5\frac{1.25^2}{s+2.5s+1.25^2}$; when fault occurs, HQ models degrade to $5\frac{1}{s+1}$ and $-2.5\frac{0.75^2}{s+1.5s+0.75^2}$ respectively.

The considered fault occurs in two actuators. Under fault-free mode, their transfer functions are:

$$A_S = A_R = \frac{25}{s+25}.$$

Two types of actuator faults are considered here: each has mean occurrence time 10^5 of FDI periods or its failure rate is 10^{-5}. Under fault type 1, the transfer function of A_S becomes

$$A'_S = 0.5\frac{15}{s+15}.$$

Under fault type 2, the transfer function of A_R becomes

$$A'_R = 0.5\frac{10}{s+10}.$$

These fault modes are described as the change of actuator gains and time constants. The set of fault modes is denoted by $S = \{0, 1, 2, 3\}$, representing fault-free, faut type 1, type 2, and simultaneous occurrence of both.

6.6.2 Performance characterization of controller and FDI

Four $\mathcal{H}_\infty$ controllers are designed for each fault mode to achieve nominal HQ control objectives under fault-free mode and degraded ones under fault modes. Typical output trajectories under fault-free mode is shown in Figure 6.3. The absolute minimal matching errors between the real responses and the ideal or degraded ones are shown in Figure 6.4, which are assumed to represent system safety behaviors. When these matching errors go over the safety limits, 30% of expected output, aircraft is considered as failed.

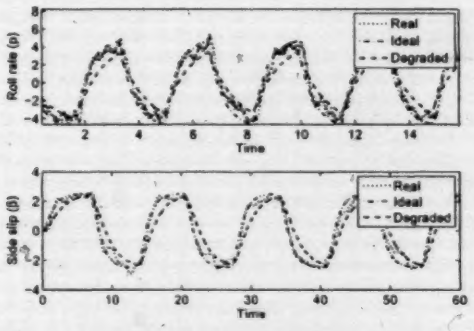

Figure 6.3: Output trajectories.

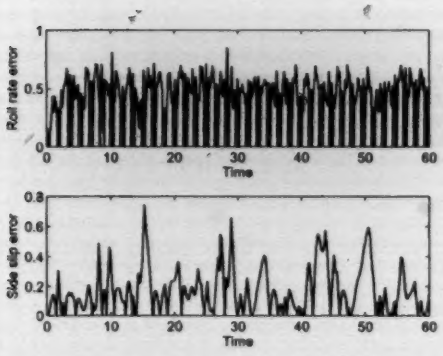

Figure 6.4: The trajectories of matching errors.

An IMM FDI was constructed to detect fault occurrences. To reduce false alarms, a steady state test strategy is applied on FDI decisions with $T_{SST_j} = 6$ for any FDI mode j. A

typical FDI trajectory is shown in Figure 6.5. It is clear that the steady FDI mode is free of false alarms in the shown time period. But detection time delays are introduced when fault occurs at 20 and 50 seconds respectively.

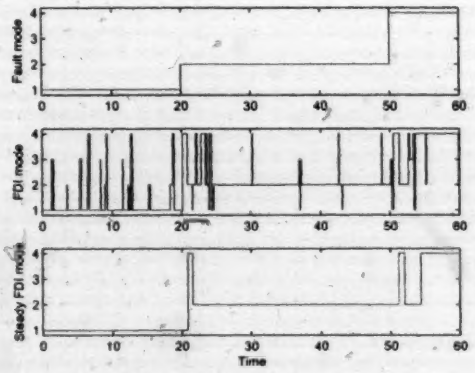

Figure 6.5: FDI trajectory.

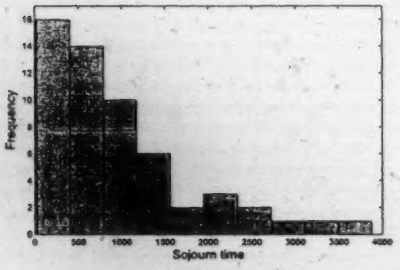

Figure 6.6: Histogram of FDI sojourn time.

To represent FDI detection characteristics, a batch of fault and FDI history data is collected for statistical estimation. First, histograms of FDI delays are generated to check its distribution type. When there is no fault, the histogram of FDI sojourn time at fault-free mode is shown in Figure 6.6. It clearly resembles a geometric distribution. Equation (6.5)-(6.6) are then used to estimate Markov transition probabilities, and those under fault-free mode are obtained as:

$$H^0 = \begin{bmatrix} 0.9990 & 0 & 0.0010 & 0.0000 \\ 1.0000 & 0 & 0 & 0 \\ 0.1330 & 0 & 0.8670 & 0 \\ 0.5000 & 0 & 0 & 0.5000 \end{bmatrix}.$$

As a result of FDI false alarms, missed detections, and detection delays, controllers may

be engaged for various fault modes for which they are not designed. So, it is necessary to evaluate system behavior under all possible combinations of FDI and fault modes. Here, Monte Carlo simulations are adopted with the following settings: 1) command stick inputs are square waves with frequency as a random variable ranging from 0.2 to 2 Hertz; 2) wind gust disturbances and sensor measurement noises are assumed to be Gaussian processes; 3) actuator saturation effects limit control inputs to 20 and 30 respectively; 4) system failure is assumed to occur when model matching errors go over 30% of stick commands. For example, with fault mode 2 occurred and $\mathcal{K}_2$ engaged, mean time to system failure is 57403 seconds when controller K_2 is used, and 6 seconds when $\mathcal{K}_1$ is used. Considering the sampling period is 0.1 second for IMM FDI, the out-crossing failure rate and hard-deadline are: $v_{22} = 1/574030,\ T_{\text{hd21}} = 60$.

6.6.3 Reliability evaluation

Reliability semi-Markov model can be constructed based on fault transition rates, FDI transition parameters, out-crossing failure rate, and hard-deadlines. Predicted reliability function and Mean Time To Failure (MTTF) can be thereby calculated. Using MTTF as an objective, an optimization is performed on T_{SST}. It is found that MTTF will be improved from 27727 to 32605 seconds if $T_{\text{SST}j}$ is reduced from 6 to 1. A comparison of reliability functions before and after this optimization is shown in Figure 6.7. It is clearly shown that reliability index is improved.

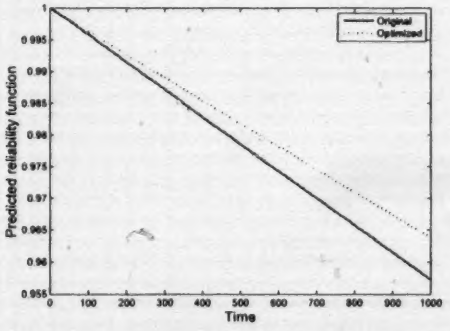

Figure 6.7: Reliability functions comparison.

Comparisons on the transition probabilities between these two SST periods are shown in Figure 6.8, in which each sub-figure gives the transition probability curves from s_{00} to other states. For example, the sub-figure at the first row and second column shows the

transition probabilities to s_{01} is increased from 0 to about 0.008. This is a natural result of increased false alarms when reducing T_{SST_j}. In fact, when $T_{SST_j} = 1$, new Markov transition parameters H'^0 becomes:

$$H'^0 = \begin{bmatrix} 0.9822 & 0.0017 & 0.0122 & 0.0038 \\ 0.2634 & 0.7366 & 0 & 0 \\ 0.1989 & 0 & 0.8011 & 0 \\ 0.3530 & 0 & 0 & 0.6470 \end{bmatrix}.$$

Compared with H^0, the element on the first row and second column is increased from 0 to 0.0017, a confirmation of increased false alarms. On the other hand, detection delays are reduced approximately from 6 to 1, and system stays less time under mis-matched fault and FDI cases. Overall, MTTF is improved.

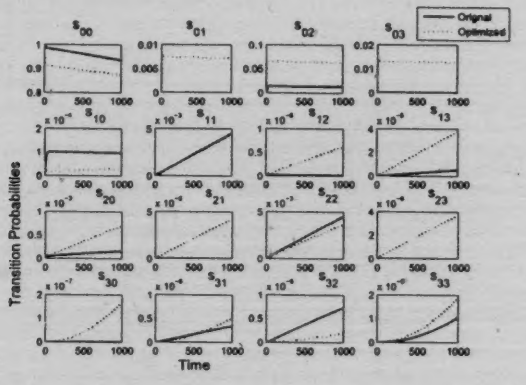

Figure 6.8: Comparison of transition probabilities.

This evaluation procedure can be completed in an online manner. Estimated FDI transition parameters H and current mode of ζ_n provided by confirmed test on FDI can be used to provide updated MTTF based on this most recent information.

6.7 Conclusions

A reliability monitoring scheme for FTCS's is reported in this chapter. The scheme contains two post-processing strategies on FDI results to provide estimated fault mode for control reconfiguration and confirmed mode for updating reliability. The stochastic transitions of FDI mode is represented by a semi-Markov chain with parameters estimated from history data. Under geometric sojourn time distributions, FDI mode can be described by an equivalent hypothetical Markov chain that simplifies its model and reliability analysis. Safety

and satisfactory operation of system is defined by system trajectories and safety boundaries; the probability of violating this safety criterion under fixed fault and FDI modes is estimated using Monte Carlo simulations. Overall reliability evaluation is obtained through a semi-Markov model constructed by integrating FDI transition characteristics and failure probabilities under each regime model. This scheme provides timely monitoring on the reliability index of FTCS's, and was demonstrated on an F-14 aircraft model.

Chapter 7

Conclusions and future work

7.1 Conclusions

This thesis discusses the analysis and design of FTCS's based on a reliability index in the following aspects:

- **Reliability analysis of FTCS's**

Constructing a reliability model is the first task in the overall framework. In the literature, Markov and semi-Markov models are commonly used to model reliability of FTCS's. Assumptions on the memory property of FDI are critical to determine model type. The states of the models are usually defined according to the combinations of the fault modes and FDI results. These available results provide some general procedures and crucial ideas for reliability analysis.

In this thesis, different from these available results, a new semi-Markov reliability model is constructed in Chapter 2 from dynamical model, and it considers some fundamental characteristics of FTCS's: control objectives, performance degradation, hard deadline in FTCS's, and effects of imperfect FDI. These aspects are incorporated in the proposed model, based on which reliability can be analyzed for FTCS's.

This analysis method also has some limitations. For example, it is developed based on two assumptions about static control performance and stationary distribution of FDI mode. It can not be applied to other control objectives defined on system transient trajectory. The approximation of stationary distribution may introduce some errors on analysis results. In addition, this method may involve heavy numerical calculation burdens.

- **Controller design based on reliability**

Once the reliability model is constructed, the reliability index is incorporated in design process, which is essentially an optimization problem with respect to a reliability

index. Owing to the numerical procedures of building and solving stochastic reliability models, reliability criteria cannot be written as analytical functions of controller parameters in general. To overcome this difficulty, based on stabilizing controller parameterization, randomization-based optimization algorithms are proposed in Chapter 3 to find the statistically optimal controller with the highest reliability. The designed controller can not only stabilize system but also achieve the optimal reliability index, such as MTTF. But this method is restricted to certain modeling structures because of the constraints on stability and parameterization results.

Another design method is given in Chapter 4 by performing MTTF optimization in two steps: 1) a gradient-based search is carried out for control performance characteristics updated along the fastest increasing direction of MTTF; 2) the updated control performance characteristics are then transmitted to a controller design algorithm, which updates controller accordingly to satisfy this performance. Each design step is completed by one iterative algorithm, and two algorithms are used alternately to complete controller design. This method helps to tackle the difficulty caused by the implicit relationship between the MTTF objective and controller parameters.

- **Improvement of FDI description and reliability modeling**

FDI is described by a Markov process in Chapters 2 through 4, and its sojourn time is exponentially distributed. However, Markov process model may not be applicable to general FDI schemes. This modeling limitation is addressed in Chapter 5 by using an extended semi-Markov description of FDI, which removes the memoryless assumption in Markov models and provides a general model for cyclic FDI schemes. Furthermore, the reliability index and evaluation method are extended to this general description of FTCS's.

- **Online reliability monitoring**

This study aims to develop online reliability monitoring scheme for active FTCS's. The reliability index can be implemented and updated online as an indication of overall system performance. It can also be used for performance analysis and design of FTCS's. The key point of online monitoring is to update reliability prediction using current available data from FDI and plant outputs. The scheme is developed mainly based on previous results in reliability modeling with necessary improvements to account for this online feature.

These reliability-based methods may be applied in the future to processes under continuous operation. To ensure productivity, operation interruptions for emergent repairs of these processes should be avoided, and they are expected to operate with satisfactory per-

formance until scheduled maintenance. The reliability-based FTC methods can be used to handle manageable faults and to retain acceptable performance. The advantage of these methods is the optimal reliability index, which can be deemed as a consistent objective of improving productivity. For some other safety-critical systems such as aircrafts, classical FTC methods may be more suitable because safety throughout each mission duration (e.g., flight time) is of top priority.

7.2 Future work

- **Calculation reduction and sensitivity analysis**

The proposed reliability is calculated from a semi-Markov model. Its calculation involves model construction and transition probability solution. Although this index may reflect characteristics of FTCS's, the complicated procedure and lack of analytical expression have caused difficulties in its applications, especially in controller design. If its calculation can be properly simplified, an approximate index may find extensive applications in both analysis and design. For example, an approximate reliability index is widely adopted in active structure control [75]. Similar idea may apply to the proposed index for FTCS's. In addition, it is worthwhile to carry out sensitivity analysis on reliability index with respect to system and probabilistic parameters to determine the effects of modeling and approximation errors.

- **Trajectory-related control objective and reliability index**

A critical issue of defining an appropriate reliability index for FTCS's is to incorporate control objective and reconfiguration actions such that this index can represent mission profile of control applications. In this thesis, reliability is defined as the probability that system satisfies a static objective. This static assumption is made based on the extensive applications of model-based control objectives and its simplicity. Model-based system norms can be used, but trajectory-based objectives are not applicable. However, it may be important to study control objectives defined on transient trajectories in some applications. An preliminary effort is made in Chapter 6 using Monte Carlo method to estimate the probability of out-crossing a safety boundary. Some design method may be developed following this idea.

- **FDI imperfectness description and FTC modeling**

FDI results provides information for controller reconfiguration, and FDI imperfectness

has been a critical issue when analyzing overall performance. In this thesis, Markov modeling is adopted. The advantage is the availability of stability results and simplicity of Markov process. But, it also has weakness on the memoryless restriction of Markov description and an appropriate selection of Markov modeling parameters. In practice, an direct description of FDI imperfectness is false alarm, missing detection, and incorrect detection probabilities. These parameters can be obtained from FDI history data. Also, many controller design techniques are a multiple-model modeling of FTCS's. It is worthwhile to extend current reliability results on these imperfectness parameters and FTC models.

- **Integrated design with maintenance activities**

Reliability problem discussed in this thesis ignored maintenance and inspection activities. If these activities are taken into account, a monitoring or prediction scheme may provide solutions for condition-based maintenance. We have made some efforts to build stochastic models for maintenance scheduling in FTCS's [95]. This method may be further improved to consider controller reconfiguration, FDI, and maintenance in a single model, which may help to design a system achieving high reliability using all available engineering activities.

- **Controller design with semi-Markov FDI description**

A semi-Markov description is more general for FDI schemes than Markov one, and a reliability index can be extended to this model. But, controller design using this modeling and reliability index is still an open problem. The difficulty lies in the stability results on this general model which may involve partial differential equations [96]. Some numerical methods may be available to solve these equations for controller design. Reliability-based design in this case may be achieved using these numerical methods.

Bibliography

[1] J. Chen and R. Patten, *Robust model-based fault diagnosis for dynamic systems*. Boston: Kluwer Academic Publisher, 1999.

[2] R. Patton, "Fault-tolerant control systems: the 1997 situation," in *IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes*, R. Patton and J. Chen, Eds. Kingston Upon Hull, UK: IFAC, 1997, vol. 3, pp. 1033–1054.

[3] D. Moerder, N. Halyo, J. Broussard, and A. Caglayan, "Application of precomputed control laws in a reconfigurable aircraft flight control system," *Journal of Guidance, Control, and Dynamics*, vol. 12, no. 3, pp. 325–333, 1989.

[4] Z. Gao and P. Antsaklis, "Reconfigurable control system design via perfect model following," *International Journal of Control*, vol. 54, no. 4, pp. 763–798, 1992.

[5] ——, "Stability of the pseudo-inverse method for reconfigurable control systems," *International Journal of Control*, vol. 53, no. 3, pp. 717–729, 1991.

[6] M. Mariton, "Detection delays, false alarm rates and the reconfiguration of control systems," *International Journal of Control*, vol. 49, pp. 981–992, 1989.

[7] M. Mahmoud, J. Jiang, and Y. Zhang, *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis*. Berlin: Springer-Verlag, 2003.

[8] Y. Zhang and J. Jiang, "Integrated active fault-tolerant control using imm approach," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 37, no. 4, pp. 1221–1235, 2001.

[9] ——, "Accepting performance degradation in fault-tolerant control system design," *IEEE Transactions on Control Systems Technology*, vol. 14, no. 2, pp. 284–292, 2006.

[10] G. Tao, S. Chen, and S. Joshi, "An adaptive control scheme for systems with unknown actuator failures," *Automatica*, vol. 38, no. 6, pp. 1027–1034, 2002.

[11] X. Zhang, T. Parisini, and M. Polycarpou, "Adaptive fault-tolerant control of nonlinear uncertain systems: an information-based diagnostic approach," *IEEE Transactions on Automatic Control*, vol. 49, no. 8, pp. 1259–1274, 2004.

[12] N. E. Wu, Y. Zhang, and K. Zhou, "Detection, estimation, and accommodation of loss of control effectiveness," *International Journal Adaptive Control Signal Processing*, vol. 14, pp. 775–795, 2000.

[13] Y. Zhang and J. Jiang, "Active fault-tolerant control system against partial actuator failures," *IEE Proceedings of Control Theory and Applactions*, vol. 149, no. 1, pp. 95–104, 2002.

[14] D. Campos-Delgado and K. Zhou, "Reconfigurable fault-tolerant control using gimc structure," *IEEE Transactions on Automatic Control*, vol. 48, no. 5, pp. 832–839, 2003.

[15] R. Srichander and B. Walker, "Stochastic stability analysis for continuous-time fault tolerant control systems," *International Journal of Control*, vol. 57, pp. 433–452, 1993.

[16] M. Mahmoud, J. Jiang, and Y. Zhang, "Stochastic stability analysis of active fault-tolerant control systems in the presence of noise," *IEEE Transactions on Automatic Control*, vol. 46, no. 11, pp. 1810–1815, 2001.

[17] F. Tao and Q. Zhao, "Stochastic fault tolerant control for optimal $\mathcal{H}_2$ performance," *International Journal of Robust and Nonlinear Control*, vol. 17, no. 1, pp. 1–24, 2007.

[18] ——, "Synthesis of fault tolerant control in the presence of random fdi delay," *International Journal of Control*, vol. 80, no. 5, pp. 684–694, 2007.

[19] R. Veillette, J. M. J, and W. Perkins, "Design of reliable control systems," *IEEE Transactions on Automatic Control*, vol. 37, no. 3, pp. 290–304, 1992.

[20] M. Blanke, M. Staroswiecki, and N. E. Wu, "Concepts and methods in fault-tolerant control," in *Proceedings of American Control Conference*, Arlington,USA, 2001, pp. 2606–2620.

[21] W. Kuo and M. Zuo, *Optimal Reliability Modeling*. Hoboken: John Wiley and Sons, 2002.

[22] N. E. Wu, "Coverage in fault-tolerant control," *Automatica*, vol. 40, pp. 537–548, 2004.

[23] N. Viswanadham, V. Sarma, and M. Singh, *Reliability of Computer and Control Systems*. Amsterdam: Elsevier science pubilishers, 1987.

[24] A. Birolini, *On the Use of Stochastic Processes in Modeling Reliability Problems*. Berlin: Springer-Verlag, 1985.

[25] E. Çinlar, *Introduction to Stochastic Processes*. Englewood Cliffs: Prentice Hall, 1975.

[26] H. Li and Q. Zhao, "A cut/tie set method for reliability evaluation of control systems," in *American Control Conference*, Portland, 2005.

[27] N. Limnios and G. Oprisan, *Semi-markov Processes and Reliability*. Boston: Birkhauser, 2001.

[28] N. E. Wu and R. Patton, "Reliability and supervisory control," in *IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes*, N. E. Wu, Ed. Washington D.C., USA: IFAC, 2003, vol. 5, pp. 1033–1054.

[29] N. E. Wu, "Reliability prediction for self-repairing flight control systems," in *Proceedings of the 35th IEEE Conference on Decision and Control*, Kobe, Japan, 1996, pp. 184–186.

[30] ——, "Reliability of fault tolerant control systems: part i and part ii," in *Proceedings of the 40th IEEE Conference on Decision and Control*, Orlando, USA, 2001, pp. 1460–1471.

[31] F. Guenab, D. Theilliol, P. Weber, J. Ponsart, and D. Sauter, "Fault tolerant control method based on cost and reliability analysis," in *The 16th IFAC World Congress*, Prague, Czech, 2005.

[32] B. Walker, "Fault tolerant control system reliability and performance prediction using semi-markov models," in *IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes*, R. Patton and J. Chen, Eds. Kingston Upon Hull, UK: IFAC, 1997, vol. 3, pp. 1053–1064.

[33] ——, "Fault detection threshold determination using markov theory," in *Fault Diagnosis in Dynamic Systems: Theory and Application*, R. Patton, P. Frank, and R. Clark, Eds. Prentice Hall, 1989.

[34] D. Schrick and P. Müller, "Reliability models for sensor fault detection with state-estimator schemes," in *Issues of Fault Diagnosis for Dynamic Systems*, R. Patton, P. Frank, and R. Clark, Eds. London: Springer-Verlog, 2000.

[35] J. Harrison, K. Daly, and E. Gai, "Reliability and accuracy prediction for a redundant strapdown navigator," *Journal of Guidance and Control*, pp. 523–529, 1981.

[36] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant control*. Berlin: Springer, 2003.

[37] F. Guenab, D. Theilliol, Y. Z. P. Weber, and D. Sauter, "Fault tolerant control system design: a reconfiguration strategy based on reliability analysis under dynamic behavior constraints," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 1387–1362.

[38] C. Bonivento, M. Capiluppi, L. Marconi, A. Paoli, and C. Rossi, "Reliability evaluation for fault diagnosis in complex systems," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 1405–1410.

[39] R. Patton, F. Uppal, S. Simani, and B. Polle, "A monte carlo analysis and design for fdi of a satellite attitude control system," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 1393–1398.

[40] N. E. Wu and S. Thavamani, "Effect of acknowledgement on performance of a fault-tolerant wireless network," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 1411–1416.

[41] J. Figueras, P. Vicencc, and J. Quevedo, "Multiple fault diagnosis system design using reliability analysis: application to barcelona rain-gauge network," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 1399–1404.

[42] M. Blanke, "Consistent design of dependable control systems," *Control Engineering Practice*, vol. 4, no. 9, pp. 1305–1312, 1996.

[43] W. Goble, *Control Systems Safety and Reliability*. Research Triangle Park: Instrument Society of America, 1998.

[44] B. Spencer, M. S. C. Won, D. Kaspari, and P. Sain, "Reliability-based measures of structural control robustness," *Structural safety*, vol. 15, pp. 111–129, 1994.

[45] K. Shin and H. Kim, "Derivation and application of hard deadlines for real-time control systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 22, no. 6, pp. 1403–1412, 1992.

[46] R. Tempo, E. Bai, and F. Dabbene, "Probabilistic robustness analysis: explicit bounds for the minimum number of samples," *Systems & Control Letters*, vol. 30, no. 5, pp. 237–242, 1997.

[47] G. Balas, A. Packard, J. Renfrow, C. Mullaney, and R. M'Closkey, "Control of the f-14 aircraft lateral-directional axis during, powered approach," *Journal of Guidance, Control, and Dynamics*, vol. 21, no. 6, pp. 899–908, 1998.

[48] B. Polyak and R.Tempo, "Probabilistic robust design with linear quadratic regulators," *Systems and Control Letters*, vol. 43, pp. 343–353, 2001.

[49] I. Yaesh, S. Boyarski, and U. Shaked, "Probability-guaranteed robust $\mathcal{H}_\infty$ performance analysis and state-feedback design," *Systems & Control Letters*, vol. 48, no. 5, pp. 351–364, 2003.

[50] G. Ciardo, R. Marie, B. Sericola, and K. Trivedi, "Performability analysis using semi-markov reward processes," *IEEE Transactions on Computers*, vol. 39, no. 10, pp. 1251–1264, 2001.

[51] Y. Fang and K. Loparo, "Stabilization of continuous-time jump linear systems," *IEEE Transactions on Automatic Control*, vol. 47, no. 10, pp. 1590–1643, 2002.

[52] L. Ghaoui and M. Ati-Rami, "Robust state-feedback stabilization of jump linear systems via lmis," *International Journal of Robust and Nonlinear Control*, vol. 6, no. 9-10, pp. 1015–1022, 1996.

[53] Y. Ji and H. Chizeck, "Controllability, stabilizability, and continuous-time markovian jump linear quadratic control," *IEEE Transactions on Automatic Control*, vol. 35, no. 7, pp. 777–788, 1990.

[54] V. Ugrinovskii, "Randomized algorithms for robust stability and guaranteed cost control of stochastic jump parameter systems with uncertain switching policies," *Journal of Optimization Theory and Applications*, vol. 124, pp. 227–245, 2005.

[55] M. Fragoso and O. Costa, "Mean square stabilizability of continuous-time linear systems with partial information on the markovian jumping parameters," *Stochastic Analysis and Applications*, vol. 22, no. 1, pp. 99–111, 2004.

[56] A. Samir, J. Christophe, and S. Dominique, "Output feedback stochastic stabilization of active fault tolerant control systems: Lmi formulation," in *16th IFAC World Congress*, Prague, 2005.

[57] F. Tao and Q. Zhao, "Design of stochastic fault tolerant control of $\mathcal{H}_2$ performance," in *Proceeding of Joint 44th IEEE Conference on Decision Control and European Control Conference*, Seville, Spain, 2005.

[58] L. Hu, P. Shi, and B. Huang, "$\mathcal{H}_\infty$ control for sampled-data linear systems with two markov processes," *Optimal Control Applications and Methods*, vol. 26, pp. 291–306, 2005.

[59] K. Zhou and J. Doyle, *Essentials of Robust Control*. Upper Saddle River: Prentice Hall, 1997.

[60] J. Doyle, K. Glover, P. Khargonekar, and B. Francis, "State-space solutions to standard $\mathcal{H}_2$ and $\mathcal{H}_\infty$ control problems," *IEEE Transactions on Automatic Control*, vol. 34, no. 8, pp. 831–847, 1989.

[61] P. Gahinet, "A new parameterization of $\mathcal{H}_\infty$ suboptimal controllers," *International Journal of Control*, vol. 59, no. 4, pp. 1031–1051, 1994.

[62] T. Iwasaki and R. Skelton, "All controllers for the general $\mathcal{H}_\infty$ control problems: Lmi existence conditions and state space formulas," *Automatica*, vol. 30, no. 8, pp. 1307–1317, 1994.

[63] R. Skelton and T. Iwasaki, "Liapunov and convariance controllers," *International Journal of Control*, vol. 57, no. 3, pp. 519–536, 1993.

[64] R. Skelton, T. Iwasaki, and K. Grigoriadis, *A Unified Approach to Linear Control Design*. London: Taylor & Francis, 1997.

[65] T. Iwasaki and R. Skelton, "Parameterization of all stabilizing controllers via quadratic lyapunov functions," *Journal of Optimization Theory and Applications*, vol. 85, no. 2, pp. 291–307, 1995.

[66] S. Boyd, L. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia: SIAM, 1994.

[67] G. Calafiore, F. Dabbene, and R. Tempo, *Randomized Algorithms for Analysis and Control of Uncertain Systems*. London: Springer-Verlag, 2005.

[68] J. do Val, J. Geromel, and A. Gonçalves, "The $\mathcal{H}_2$-control for jump linear systems: cluster observations of the markov state," *Automatica*, vol. 38, pp. 343–349, 2002.

[69] M. Mahmoud, J. Jiang, and Y. Zhang, "Stabilization of active fault tolerant control systems with imperfect fault detection and diagnosis," *Stochastic Analysis and Applications*, vol. 21, no. 3, pp. 673–701, 2003.

[70] H. Li and Q. Zhao, "Analysis of fault tolerant control by using randomized algorithms," in *Prococeeding of American Control Conference*, Portland, USA, 2005.

[71] P. Gahinet, A. Nemirovski, A. Laub, and M. Chilali, *LMI Control Toolbox User's Guide*. The MathWorks, 2005.

[72] S. Ross, *Introduction to probability models*, 6th ed. San Diego: Academic Press, 1997.

[73] R. Isermann, "Model-based fault-detection and diagnosis - status and applications," *Annual Reviews in Control*, vol. 29, pp. 71–85, 2005.

[74] A. Doucet and C. Andrieu, "Iterative algorithms for state estimation of jump markov linear systems," *IEEE Transactions on Signal Processing*, vol. 49, no. 5, pp. 1216–1227, 2001.

[75] R. Field and L. Bergman, "Reliability-based approach to linear covariance control design," *Journal of Engineering Mechanics*, vol. 124, no. 2, pp. 193–199, 1998.

[76] F. Guenab, D. Theillol, P. Weber, Y. Zhang, and D. Sauter, "Fault tolerant control system design: a reconfiguration strategy based on reliability analysis under dynamic behavior constraint," in *Proceedings of Safeprocess*, Beijing, China, 2006, pp. 1387–1392.

[77] G. Calafiore and B. Polyak, "Stochastic algorithms for exact and approximate feasibility of robust lmis," *IEEE Transactions on Automatic Control*, vol. 46, no. 11, pp. 1755–1759, 2001.

[78] Y. Fujisaki, F. Dabbene, and R. Tempo, "Probabilistic robust design of lpv control systems," *Automatica*, vol. 39, no. 8, pp. 1323–1337, 2003.

[79] D. Liberzon and R. Tempo, "Gradient algorithms for finding common lyapunov functions," in *Proceedings of the 42nd IEEE Conference on Decision and Control*, Hawaii, USA, 2003, pp. 4782–4786.

[80] A. Skovrokhod, *Asymptotic Methods in the Theory of Stochastic Differential Equations*. Providence: American Mathematical Society, 1989.

[81] W. Wonham, "Random differential equations in control theory," in *Probabilistic Methods in Applied Mathematics*, A. Bharucha-Reid, Ed. New York: Academic Press, 1970.

[82] X. M. X and C. Yuan, *Stochastic Differential Equations with Markovian Switching*. London: Imperial College Press, 2006.

[83] J. Hu, C. Bohn, and H. Wu, "Systematic weighting function selection and its application to the real-time control of a vertical take-off aircraft," *Control Engineering Practice*, vol. 8, no. 3, pp. 241–252, 2000.

[84] G. Dullerud and F. Paganini, *A Course in Robust Control Theory: a Convex Approach*. New York: Springer-Verlag, 2000.

[85] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York: Cambridge University Press, 2004.

[86] N. Shor, *Minimization Methods for Non-Differentiable Functions*. Berlin: Spring-Verlag, 1985.

[87] M. Mahmoud, "Continuously variable duration markov models for detection delays in linear jump systems," in *Proceedings of American Control Conference*, Denver, USA, 2003, pp. 4851–4856.

[88] W. Kuo and M. Zuo, *Optimal Reliability Modeling*. Hoboken, USA: John Wiley and Sons, 2002.

[89] N. Viswanadham, V. Sarma, and M. Singh, *Reliability of Computer and Control Systems*. New York: Elisevier Science, 1987.

[90] V. Barbu, M. Boussemart, and N. Limnios, "Discrete-time semi-markov model for reliability and survival analysis," *Communications in Statistics Theory and Methods*, vol. 33, no. 11, pp. 2833–2868, 2004.

[91] R. Howard, *Dynamic Probabilistic Systems*. New York: Wiley, 1971, vol. II.

[92] Y. Zhang and J. Jiang, "Active fault-tolerant control system against partial actuator failures," *IEE Proceedings on Control Theory and Applications*, vol. 149, no. 1, pp. 95–104, 2002.

[93] J. Song and A. Kiureghian, "Joint first-passage probability and reliability of systems under stochastic excitation," *Journal of Engineering Mechanics*, vol. 132, no. 1, pp. 65–77, 2006.

[94] Y. Zhang and X. Li, "Detection and diagnosis of sensor and actuator failures using IMM estimator," *IEEE Transactions on Aerospace Electronic Systems*, vol. 34, no. 4, pp. 1293–1313, 1998.

[95] H. Li and Q. Zhao, "Maintenance modeling and scheduling in fault tolerant control systems," in *Proceedings of Safeprocess*, Beijing, 2006, pp. 829–834.

[96] D. Sworder, "Control of a linear system with non-markovian modal changes," *Journal of Economic Dynamics and Control*, vol. 2, pp. 233–240, 1980.

Appendix A

Semi-Markov processes

Let X_n represent a random variable defined in a countable set E, and T_n defined in R_+ such that $0 = T_0 \leq T_1 \leq T_2 \leq \cdots, n \in \mathbb{N}$.

Definition A.1 *$(X,T) = \{X_n, T_n : n \in N\}$ is said to be a Markov renewal process with state space E provided that*

$$Pr\{X_{n+1} = j, T_{n+1} - T_n \leq t | X_0, \cdots, X_n : T_0, \cdots, T_n\} = Pr\{X_{n+1} = j, T_{n+1} - T_n \leq t | X_n\},$$

for all $n \in N, j \in E$ and $t \in R_+$. (X,T) is time-homogeneous, if, for any $i, j \in E, t \in R_+$,

$$Pr\{X_{n+1} = j, T_{n+1} - T_n \leq t | X_n = i\} = Q(i,j,t),$$

independent of n. $Q = \{Q(i,j,t) : i, j \in E, t \in R_+\}$ is called a semi-Markov kernel over E.

Let $P(i,j) \triangleq \lim_{t\to\infty} Q(i,j,t)$. It can be shown that $P(i,j) \geq 0$ and $\sum_{j\in E} P(i,j) = 1$ [25, 27]. So, $P(i,j)$ is the transition probability for some Markov chain with sate space E. As $\Pr\{X_{n+1} = j | X_0, \cdots, X_n; T_0, \cdots, T_n\} = P(X_n, j)$ for $n \in N, j \in E$, $X = \{X_n : n \in N\}$ is a Markov chain with state space E and transition matrix P.

The expectation of the sojourn time in state i, or the mean sojourn time $m(i)$, can be calculated by following equation.

$$m(i) = \int_0^\infty (1 - \sum_k Q(i,k,t))dt. \tag{A.1}$$

For convenience, denote $\Pr\{\cdot | X_0 = i\}$ as $\Pr_i$. Define $Q^n(i,j,t) = \Pr_i\{X_n = j, T_n \leq t\}, i, j \in E, t \in R_+$, then

$$Q^0(i,j,t) = \delta(i,j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

$Q^{n+1}(i,k,t)$ can be defined recursively as

$$Q^{n+1}(i,k,t) = \sum_{j \in E} \int_0^t Q(i,j,ds) Q^n(j,k,t-s), \tag{A.2}$$

which is the $(n+1)$-order Stieltjes convolution in matrix form.

The following equation gives the Markov renewal function, which plays an important role in the calculation of transition probability.

$$\begin{aligned} R(i,j,t) &= \sum_{n=0}^{\infty} \Pr\{X_n = j, T_n \leq t\} \\ &= \sum_{n=0}^{\infty} Q^n(i,j,t). \end{aligned} \tag{A.3}$$

Define $L = Sup_n T_n$, the life time of Markov renewal process (X,T). To extend the definition to t beyond L, define

$$Y_t = \begin{cases} X_n, & \text{if } T_n \leq t < T_{n+1}, \\ \Upsilon, & \text{if } t \geq L. \end{cases}$$

where Υ is not a elment of E. Then, $Y = \{Y_t, t \geq 0\}$ is called minimal semi-Markov process associated with (X,T). Please note that if E is a finite set, $L = \infty$ and there is no need for Υ.

As in the analysis of Markov processes, the most important parameter is the transition probability $P_t(i,j) = \Pr_i(Y_t = j)$. It can been proved that the transition probability can be computed by the following integration [25].

$$P_t(i,j) = \int_0^t R(i,j,ds) h(j,t-s), \tag{A.4}$$

where $h(j,t) = 1 - \sum_{k \in E} Q(j,k,t), j \in E, t \geq 0$.

Appendix B

Reliability calculation from semi-Markov process model

Let $X^{\mathrm{R}}(t)$ represents a semi-Markov reliability model. Its state space are classified into two complementary sets: let M represent the set of up states and $\bar{M}$ for down states. When $X^{\mathrm{R}}(t) \in M$, the system is considered to be functional; otherwise, nonfunctional.

If the down states in $\bar{M}$ are absorbing, the reliability function can be calculated from the transition probability. Assume that $\Pr\{X(0) = i\} = P_0(i)$, then

$$\begin{aligned} R(t) &= \Pr\{\forall u \in [0,t], X(u) \in M\} \\ &= \Pr\{X^{\mathrm{R}}(t) \in M\} \\ &= \sum_{i \in M} \sum_{j \in M} \Pr\{X^{\mathrm{R}}(t) = j | X(0) = i\} \Pr\{X(0) = i\} \\ &= \sum_{i \in M} \sum_{j \in M} P_0(i) P_t(i,j). \end{aligned} \tag{B.1}$$

In case that the down states are not absorbing, an auxiliary semi-Markov process can be constructed from which the reliability of the original process can be calculated using the above equation.

MTTF is the expectation of the life time of the item[23, 27]. Denote m_0 as the vector of mean sojourn time in the up states and partition the transition probability matrix P of the embedded Markov chain as:

$$P = \begin{bmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{bmatrix}.$$

If $I - P_{00}$ is non-singular, MTTF= $P_0(I - P_{00})^{-1} m_0$.